Manuel de l'utilisateur de HP Integrated Lights-Out 2

Pour microprogrammes 1.75 et 1.77



Référence 394326-059

Avril 2009 (Neuvième édition)

Public visé

Ce manuel est destiné au personnel qui installe, administre et répare les serveurs et systèmes de stockage. HP suppose que vous êtes qualifié en réparation de matériel informatique et que vous êtes averti des risques inhérents aux produits capables de générer des niveaux d'énergie élevés.

Sommaire

1 Présentation du fonctionnement

Cette section traite des rubriques suivantes :

Présentation du manuel

HP iLO 2 offre de nombreuses méthodes de configuration, de mise à jour et d'utilisation des serveurs à distance. Le *Manuel de l'utilisateur de HP Integrated Lights-Out 2* décrit ces fonctions et leur fonctionnement avec l'interface basée sur le navigateur et l'utilitaire RBSU. Certaines de ces fonctions sont sous licence et uniquement accessibles après l'achat de celle-ci. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21).

Le *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out* décrit la syntaxe et les outils disponibles pour utiliser la carte iLO 2 via une ligne de commande ou une interface de scripts.

Le présent manuel décrit la carte HP Integrated Lights-Out pour les serveurs ProLiant ML/DL, ainsi que les lames de serveur ProLiant BladeSystem. Pour obtenir des informations sur iLO pour les serveurs et lames de serveur Integrity, reportez-vous au site Web HP (http://www.hp.com/go/integrityiLO).

Ce manuel contient des informations concernant le microprogramme iLO 2 versions 1.11, 1.2x, 1.3x, 1.70, 1.75 et 1.77.

Nouveautés de cette version de iLO 2

iLO 2 version 1.77 ajoute une prise en charge pour un usage amélioré au travers de l'utilisation d'un mode HEM (High Efficiency Mode – Mode haute efficacité). Pour plus d'informations, reportez-vous à la section « Efficacité de l'alimentation » (Efficacité de l'alimentation à la page 134).

Nouvelles fonctions prises en charge par iLO 2 version 1,75 :

- Prise en charge de modèles de licence : iLO 2 propose des licences iLO Advanced et iLO Advanced pour BladeSystem en tant que mises à niveau pouvant être achetées pour les fonctions de supervision distante standard disponibles sur vos systèmes HP ProLiant et BladeSystem. Pour plus d'informations, consultez le site Web HP (http://www.hp.com/go/ilo).
- Prise en charge améliorée de comptes d'annuaire pour jusqu'à 15 contextes de recherche.
- Prise en charge de services d'annuaire pour Windows 2008 Active Directory.

- Génération de rapports d'état de température, lorsque pris en charge par la plateforme.
- Serveurs supplémentaires :
  - ProLiant BL260c G6
  - ProLiant BL460c G6
  - ProLiant BL490c G6
  - ProLiant DL320 G6
  - ProLiant DL360 G6
  - ProLiant DL380 G6
  - ProLiant ML310 G5p
  - ProLiant ML330 G6
  - ProLiant ML350 G6
  - ProLiant ML370 G6

Présentation de iLO 2

iLO 2 peut effectuer à distance la plupart des fonctionnalités nécessitant une intervention sur les serveurs au niveau du centre de données, de la salle des ordinateurs ou de l'emplacement distant. Voici quelques exemples d'utilisation des fonctions de iLO2.

- La console distante iLO 2 et l'alimentation virtuelle permettent de visualiser un serveur distant bloqué avec des conditions d'écran bleu et de redémarrer le serveur sans assistance sur site.
- La console distante iLO 2 permet de modifier des paramètres BIOS si nécessaire.
- La technologie iLO 2 Virtual KVM fournit une console distante hautes performances qui permet d'administrer à distance des systèmes d'exploitation et des applications dans des situations de tous les jours.
- Un lecteur virtuel de CD/DVD-ROM ou de disquette iLO 2 permet d'installer un système d'exploitation ou un microprogramme de système flash sur le réseau à partir d'images sur des stations de travail ou des serveurs Web centralisés.
- iLO 2 Virtual Folder (Dossier virtuel) permet de mettre à jour les drivers du système d'exploitation ou de copier des fichiers système sans support physique ou sans créer d'image du disque.
- La fonction de script iLO 2 permet d'utiliser des possibilités d'alimentation virtuelle et de support virtuel dans d'autres outils de script afin d'automatiser le déploiement et le provisionnement.
- iLO 2 participe activement à la surveillance de l'état du serveur (état intégré) et à sa maintenance. Il surveille les températures au sein du serveur et envoie des signaux correcteurs aux ventilateurs afin que ces derniers assurent le niveau de refroidissement requis. iLO 2 permet en outre de surveiller l'état des ventilateurs, des alimentations, des régulateurs de tension et des disques durs internes.

Ceci ne constitue que quelques exemples de la manière dont iLO 2 peut être utilisé pour gérer des serveurs HP ProLiant depuis votre bureau, votre maison ou lorsque vous êtes en déplacement. Au fur et à mesure que vous utilisez iLO 2 et que vous définissez les besoins spécifiques de votre infrastructure, ce guide vous fournira des moyens supplémentaires vous permettant de simplifier la supervision de vos serveurs distants.

Pour obtenir des informations concernant les fonctions proposées par chacune des versions d'iLO 2, reportez-vous à la section « Licence » (Licence à la page 21).

Différences entre iLO 2 et iLO

iLO 2 est basé sur iLO et propose de nombreuses fonctions communes. Cependant, si iLO 2 est utilisé pour accéder à une console distante texte avec pré-système d'exploitation, vous devez utiliser la console série distante. Pour plus d'informations, reportez-vous à la section « Présentation de la console distante texte » (Présentation de la console distante texte à la page 107).

Le tableau ci-dessous présente les différences entre iLO 2 et iLO :

Élément	iLO 2	iLO
Fonctions standard		
Console texte	Pré-SE	Pré-SE ou SE
Remote Serial Console (Console série distante - port série virtuel)	Pré-SE ou SE	Pré-SE ou SE
Surveillance de l'état du serveur et maintenance	Oui	Non
Fonctions avancées		
Console texte	Pré-SE ou SE	Pré-SE ou SE
Remote console (Console distante)	Oui (Virtual KVM)	Oui
Integrated Remote Console (Console distante intégrée)	Oui	Non
Prise en charge de Microsoft® JVM	Oui	Non
Bouton Remote Console Acquire (Acquisition de console distante)	Oui	Oui
Intégration de Terminal Services	Oui	Oui
Intégration d'annuaire, dans le cadre du schéma HP	Oui	Oui
Intégration d'annuaire sans schéma	Oui	Oui
Authentification à deux facteurs	Oui	Oui
Rapports du régulateur de puissance	Oui	Oui
Disquette et CD/DVD-ROM virtuels	Oui	Oui
Support virtuel de clés USB	Oui	Oui
Virtual Folder (Dossier virtuel)	Oui	Non

Intégration du HP Insight Essentials Rapid Deployment Pack

Le pack HP Insight Essentials Rapid Deployment Pack (Pack de déploiement rapide HP Insight Essentials) s'intègre avec la carte iLO 2 pour permettre la gestion des serveurs distants et des performances des opérations de la console distante, indépendamment de l'état du système d'exploitation ou du matériel.

Le serveur de déploiement permet d'utiliser les fonctions de gestion de l'alimentation de la carte iLO 2 pour la mise sous tension, la mise hors tension et la réinitialisation sur le serveur cible. Chaque fois que le serveur se connecte sur la fonctionnalité Deployment Server, cette dernière interroge le serveur cible pour vérifier si un périphérique de supervision LOM est installé. Le cas échéant, le serveur collecte les informations, notamment le nom DNS, l'adresse IP et le premier nom utilisateur. La sécurité est maintenue grâce à l'invite, faite à l'utilisateur, d'entrer le mot de passe correct pour ce nom utilisateur.

Pour plus d'informations sur le pack HP Insight Essentials Rapid Deployment Pack, reportez-vous à la documentation disponible sur le CD correspondant ou sur le site Web HP (http://www.hp.com/servers/rdp).

Supervision de serveur via les applications compatibles IPMI version 2.0

La supervision de serveur via IPMI est une méthode normalisée de contrôle et de surveillance du serveur. iLO 2 fournit les fonctions de supervision de serveur conformément à la spécification IPMI version 2.0.

La spécification IPMI définit une interface normalisée pour la gestion de plate-forme. La spécification IPMI définit les types de supervision de plate-forme suivants :

- Supervision des informations système, relatives notamment aux ventilateurs, aux températures et aux blocs d'alimentation
- Fonctions de récupération, telles que les réinitialisations et les opérations de mise sous tension/hors tension du système
- Fonctions de consignation, pour les événements anormaux tels que les relevés de températures excessives ou les pannes de ventilateur
- Fonctions d'inventaire, telles que l'identification des composants matériels en panne

Les communications IPMI dépendent des fonctions BMC et SMS. BMC supervise l'interface entre SMS et le matériel de supervision de plate-forme. iLO 2 émule la fonctionnalité BMC, tandis que la fonctionnalité SMS peut être fournie par différents outils aux normes du marché. Pour plus d'informations, reportez-vous à la spécification IPMI sur le site Web Intel® (http://www.intel.com/design/servers/ipmi/tools.htm).

iLO 2 fournit l'interface KCS, ou interface ouverte, pour les communications SMS. L'interface KCS fournit un ensemble de registres de communications d'E/S associées. L'adresse de base du système par défaut pour l'interface SMS d'E/S associée est 0xCA2 et est alignée sur l'octet au niveau de cette adresse système.

L'interface KCS est accessible au logiciel SMS en cours d'exécution sur le système local. Exemples d'applications logicielles SMS compatibles :

- L'outil Command Test de IPMI version 2.0 est un outil de ligne de commande MS-DOS de bas niveau permettant l'envoi des commandes IPMI au format hexadécimal à une fonction BMC IPMI qui met en œuvre l'interface KCS. Vous trouverez cet outil sur le site Web Intel® (http://www.intel.com/design/servers/ipmi/tools.htm).
- IPMItool est un utilitaire de supervision et de configuration des périphériques prenant en charge les spécifications des versions 1.5 et 2.0 de IPMI ; il peut être utilisé dans un environnement Linux. Vous trouverez cet outil sur le site Web IPMItool (http://ipmitool.sourceforge.net/index.html).

Fonctionnalité IPMI fournie par iLO 2

Lors de l'émulation d'une fonction BMC pour l'interface IPMI, iLO 2 prend en charge toutes les commandes obligatoires répertoriées dans la spécification IPMI version 2.0. Pour obtenir la liste de ces commandes, reportez-vous à la spécification IPMI version 2.0. En outre, SMS doit utiliser les méthodes

décrites dans la spécification pour la détermination des fonctions IPMI activées ou désactivées dans BMC (par exemple, utilisation de la commande Get Device ID [Obtenir l'ID de périphérique]).

Si le système d'exploitation du serveur est en cours d'exécution et que le driver d'état est activé, n'importe quel trafic IPMI via l'interface KCS peut affecter les performances du driver d'état et les performances d'état globales du système. Ne saisissez pas de commandes IPMI via l'interface KCS car cela peut avoir un effet négatif sur la surveillance effectuée par le driver d'état. Ces commandes incluent toute commande définissant ou modifiant les paramètres IPMI, tels que `Set Watchdog Timer` et `Set BMC Global Enabled`. Les commandes IPMI qui ne renvoient que des données peuvent être utilisées en toute sécurité comme, par exemple, `Get Device ID` et `Get Sensor Reading`.

Présentation de la compatibilité WS-Management

La mise en œuvre du microprogramme iLO 2 de WS-Management est conforme à la spécification DTMF *Web Services for Management* 1.0.0a.

Authentification

- iLO 2 utilise une authentification SSL de base, compatible avec le profil : `wsman:secprofile/https/basic`
- Les utilisateurs authentifiés sont autorisés à exécuter les commandes WS-Management en fonction des privilèges attribués à leur compte local ou d'annuaire.
- Pour activer une authentification de base sous Microsoft® Windows Vista™, saisissez `gpedit.msc` à l'invite pour lancer l'Éditeur d'objets de stratégie de groupe. Sélectionnez **Configuration ordinateur>Modèles d'administration>Composants Windows>Gestion à distance de Windows (WinRM)>Client WinRM**. Cochez la case permettant d'autoriser l'authentification de base.

Compatibilité

- WS-Management d'iLO 2 est compatible avec l'utilitaire WinRM de Windows Vista™, Microsoft® Operations Manager 3 et le Management Pack fourni par HP.
- L'ensemble des commandes WS-Management est disponible sur les serveurs iLO 2 prenant en charge l'état du système intégré. Une très petite partie de ces commandes est disponible sur les serveurs ne prenant pas en charge l'état des systèmes intégrés.

Ces commandes peuvent être utilisées pour une invocation distante des équipements suivants :

- Alimentation du serveur
- UID

État

WS-Management de iLO 2 renvoie des informations concernant les températures, l'état des ventilateurs, des blocs d'alimentation et des VRM.

Présentation de l'interface du navigateur iLO 2

L'interface du navigateur iLO 2 regroupe des tâches semblables afin de faciliter la navigation et le flux de travail. Ces tâches sont divisées en onglets de haut niveau situés dans la partie supérieure de l'interface de iLO 2. Ces onglets sont toujours visibles et incluent System Status (État du système), Remote Console (Console distante), Virtual Media (Support virtuel), Power Management (Gestion de l'alimentation) et Administration.

Chaque onglet iLO 2 de haut niveau possède un menu sur le côté gauche de l'interface avec diverses options. Ce menu change à chaque sélection d'un onglet de haut niveau différent et affiche les options

correspondantes. Chaque option de menu affiche un titre de page. Celui-ci décrit les informations ou les paramètres disponibles sur cette page. Le titre de la page peut ne pas correspondre au nom de l'option de menu.

Une assistance pour toutes les pages iLO 2 est disponible dans l'aide en ligne. Les liens sur chaque page iLO 2 fournissent des informations récapitulatives sur les fonctions iLO 2 et des informations utiles pour optimiser leur fonctionnement. Pour accéder à une page d'aide spécifique, cliquez sur le **point d'interrogation (?)** dans la partie droite de la fenêtre du navigateur.

Les tâches utilisateur typiques sont disponibles dans les onglets System Status (État du système), Remote Console (Console distante), Virtual Media (Support virtuel) et Power Management (Gestion de l'alimentation) de l'interface iLO 2. Ces tâches sont décrites dans la section « Utilisation de iLO 2 » (Utilisation de iLO 2 à la page 81).

L'onglet Administration est, en général, utilisé par un administrateur ou un utilisateur avancé pour gérer les utilisateurs, configurer les paramètres globaux et du réseau ainsi que pour configurer ou activer les fonctions les plus avancées d'iLO 2. Ces tâches sont présentées aux sections « Installation de iLO 2 » (Installation de iLO 2 à la page 9) et « Configuration de iLO 2 » (Configuration de iLO 2 à la page 18).

Certaines particularités des fonctions et de l'intégration de iLO 2 sont détaillées dans les sections suivantes :

- Services d'annuaire (Services d'annuaire à la page 149)
- Supervision distante activée via l'annuaire (Supervision distante activée via l'annuaire à la page 184)
- Utilitaire de migration d'annuaire HPQLOMIG (Utilitaire de migration d'annuaire HPQLOMIG à la page 192)
- Intégration de HP SIM (Systems Insight Manager) (Intégration de HP SIM (Systems Insight Manager) à la page 204)
- Résolution des problèmes de la carte iLO 2 (Résolution des problèmes de la carte iLO 2 à la page 210)
- Schéma des services d'annuaire (Schéma des services d'annuaire à la page 238)

Navigateurs et systèmes d'exploitation client pris en charge

- Microsoft® Internet Explorer 7
  - Ce navigateur est pris en charge sur les produits Microsoft® Windows®.
  - HP prend en charge Microsoft® JVM et SUN Java™ 1.4.2_13. Pour télécharger la machine virtuelle Java recommandée pour votre configuration système, reportez-vous au site Web HP (http://www.hp.com/servers/manage/jvm).
- Microsoft® Internet Explorer 6 avec Service Pack 1 ou version supérieure
  - Ce navigateur est pris en charge sur les produits Microsoft® Windows®.
  - HP prend en charge Microsoft® JVM et SUN Java™ 1.4.2_13. Pour télécharger la machine virtuelle Java recommandée pour votre configuration système, reportez-vous au site Web HP (http://www.hp.com/servers/manage/jvm).
- Firefox 2.0
  - Ce navigateur est pris en charge sur Red Hat Enterprise Linux Desktop 4 et Novell Linux Desktop 9.
  - HP prend en charge Microsoft® JVM et SUN Java™ 1.4.2_13. Pour télécharger la machine virtuelle Java recommandée pour votre configuration système, reportez-vous au site Web HP (http://www.hp.com/servers/manage/jvm).

Certaines combinaisons de navigateurs et de systèmes d'exploitation peuvent ne pas fonctionner correctement, selon la manière dont ces derniers mettent en œuvre les technologies de navigation requises.

Systèmes d'exploitation serveur pris en charge

iLO 2 est un microprocesseur indépendant qui exécute un système d'exploitation intégré. Cette architecture garantit la disponibilité de la plupart des fonctions de iLO 2, indépendamment du système d'exploitation hôte utilisé.

Pour que les opérations de fermeture du système d'exploitation s'effectuent dans les règles, l'intégration avec HP SIM nécessite des drivers d'état et des agents de supervision, ou l'accès à la console distante.

iLO 2 fournit deux drivers d'interface :

- Le driver de contrôleur iLO 2 ASM (Advanced System Management) permet d'assurer la supervision des systèmes, notamment la surveillance des composants serveur, la consignation des événements et la prise en charge des agents de supervision.
- iLO 2 Management Interface Driver permet au logiciel du système et aux agents SNMP Insight de communiquer avec iLO 2.

Ces drivers et ces agents sont disponibles pour les systèmes d'exploitation réseau suivants :

- Microsoft®
  - Windows® 2008 Server
  - Windows® 2008 Advanced Server
  - Windows Server® 2003
  - Windows Server® 2003, Web Edition

- Windows® Small Business Server 2003 (gamme ML300)
- Windows Vista®

- Red Hat
  - RedHat Enterprise Linux 3 (x86)
  - RedHat Enterprise Linux 3 (AMD64/EM64T)
  - RedHat Enterprise Linux 4 (x86)
  - RedHat Enterprise Linux 4 (AMD64/EM64T)
  - RedHat Enterprise Linux 5 (x86)
  - RedHat Enterprise Linux 5 (AMD64/EM64T)
- SUSE
  - SUSE LINUX Enterprise Server 9 (x86)
  - SUSE LINUX Enterprise Server (AMD64/EM64T)
  - SUSE LINUX Enterprise Server 10

2 Installation de iLO 2

Cette section traite des rubriques suivantes :

Installation rapide

Afin de configurer rapidement iLO 2 à l'aide des paramètres par défaut de iLO 2 Standard et des fonctions de iLO Advanced, procédez comme suit :

1. Réfléchissez sur la façon dont vous allez gérer votre réseau et la sécurité (Préparation de l'installation de iLO 2 à la page 10).
2. Connectez iLO 2 au réseau (Connexion au réseau à la page 12).
3. Si vous ne faites pas appel à l'adressage IP dynamique, utilisez l'utilitaire iLO 2 RBSU afin de configurer une adresse IP statique (Configuration de l'adresse IP à la page 12).
4. Connectez-vous à la carte iLO 2 via un navigateur compatible ou une ligne de commande à l'aide du nom d'utilisateur, du mot de passe et du nom DNS par défaut figurant sur l'étiquette iLO 2 Network Settings (Paramètres réseau iLO 2) apposée sur le serveur (Première connexion à iLO 2 à la page 13).
5. Modifiez le nom utilisateur et le mot de passe par défaut du compte administrateur pour vos sélections prédéfinies.
6. Si vous utilisez les comptes locaux, configurez les comptes de vos utilisateurs (Configuration des comptes utilisateur à la page 13).
7. Activez les fonctions avancées d'iLO 2 (Activation des fonctions sous licence de iLO 2 à l'aide d'un navigateur à la page 14).
8. Installez les drivers de périphérique iLO 2 (Installation des drivers du périphérique iLO 2 à la page 15).

Préparation de l'installation de iLO 2

Avant de configurer les processeurs de supervision iLO 2, vous devez décider de la façon dont vous allez gérer votre réseau et la sécurité. Les questions suivantes vous aideront à configurer iLO 2 selon vos besoins :

1. De quelle façon connecter iLO 2 au réseau ? Pour obtenir des informations sur les connexions disponibles et accéder à un schéma, reportez-vous à la section « Connexion au réseau » (Connexion au réseau à la page 12).

   De manière générale, iLO 2 est connecté au réseau via l'un des éléments suivants :

   ◦ Un réseau d'entreprise auquel sont connectés la carte réseau et le port iLO 2. Cette connexion permet d'accéder à iLO 2 à partir de tout endroit du réseau. Le matériel réseau et l'infrastructure nécessaires à la prise en charge de iLO 2 sont ainsi réduits. Cependant, sur ce type de réseau, les performances de iLO 2 peuvent être diminuées par le trafic.

   ◦ Un réseau de supervision dédié avec le port iLO 2 connecté à un autre réseau. Ce dernier permet d'améliorer les performances et la sécurité. En effet, vous pouvez physiquement contrôler les connexions des stations de travail au réseau. Il fournit également un accès redondant au serveur lorsqu'une panne de matériel survient sur le réseau d'entreprise. Dans cette configuration, iLO 2 n'est pas directement accessible à partir du réseau d'entreprise.

2. Comment se fait l'obtention d'une adresse IP par iLO 2 ?

   Pour accéder à iLO 2 après l'avoir connecté au réseau, le processeur de supervision doit obtenir une adresse IP et un masque de sous-réseau à l'aide d'un processus dynamique ou statique :

   ◦ Une adresse IP dynamique est définie par défaut. iLO 2 obtient l'adresse IP et le masque de sous-réseau des serveurs DNS/DHCP. Cette méthode est la plus simple.

   ◦ Une adresse IP statique permet de configurer une adresse IP du même type si les serveurs DNS/DHCP sont indisponibles sur le réseau. À l'aide de RBSU, une adresse IP statique peut être configurée sur iLO 2.

     Lorsque vous utilisez la fonction Static IP (IP statique), vous devez posséder une adresse IP avant de commencer à configurer iLO 2.

3. Quelle sécurité appliquer aux droits d'accès et quels sont les comptes utilisateur et privilèges à configurer ?

   iLO 2 offre plusieurs options concernant le contrôle des droits d'accès des utilisateurs. Pour empêcher les accès non autorisés aux ressources IT d'une entreprise, sélectionnez l'une des méthodes suivantes :

   ◦ Vous pouvez enregistrer des comptes locaux avec jusqu'à 12 noms utilisateur et mots de passe sur iLO 2. Cette méthode est idéale pour les petits environnements tels que les laboratoires et les moyennes entreprises.

   ◦ Vous pouvez utiliser l'annuaire d'entreprise (Microsoft® Active Directory ou Novell eDirectory) pour gérer l'accès des utilisateurs à iLO 2. Cette méthode est idéale pour les environnements dans lesquels les utilisateurs varient fréquemment. Si vous avez choisi d'utiliser les services d'annuaire, laissez au moins un compte local actif pour vous donner un autre accès.

     Pour plus d'informations concernant la sécurité de l'accès à iLO 2, reportez-vous à la section « Sécurité » (Sécurité à la page 40).

4. Quelle configuration de iLO 2 choisir ?

iLO 2 prend en charge diverses interfaces pour la configuration et l'exploitation. Le présent manuel décrit en détails les interfaces suivantes :

◦ L'utilitaire iLO 2 RBSU (Installation de iLO 2 à l'aide de iLO 2 RBSU à la page 14) peut être employé lorsque l'environnement système n'utilise pas de serveur DHCP, DNS ou WINS.

◦ La méthode d'installation basée sur le navigateur (Installation de iLO 2 à l'aide de l'option basée sur le navigateur à la page 14) convient lorsque vous pouvez vous connecter à iLO 2 sur le réseau via un navigateur. Cette méthode permet également de reconfigurer iLO 2.

◦ SMASH CLP (CLP SMASH) peut être utilisé lorsque vous avez accès à une ligne de commande via Telnet, SSH ou un port série physique. Reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Les paramètres iLO 2 par défaut permettent d'utiliser la plupart des fonctionnalités sans configuration supplémentaire. Cependant, la flexibilité de la configuration de iLO 2 permet de personnaliser plusieurs environnements d'entreprise. Pour obtenir la liste complète des options disponibles, reportez-vous à la section « Configuration de iLO 2 » (Configuration de iLO 2 à la page 18).

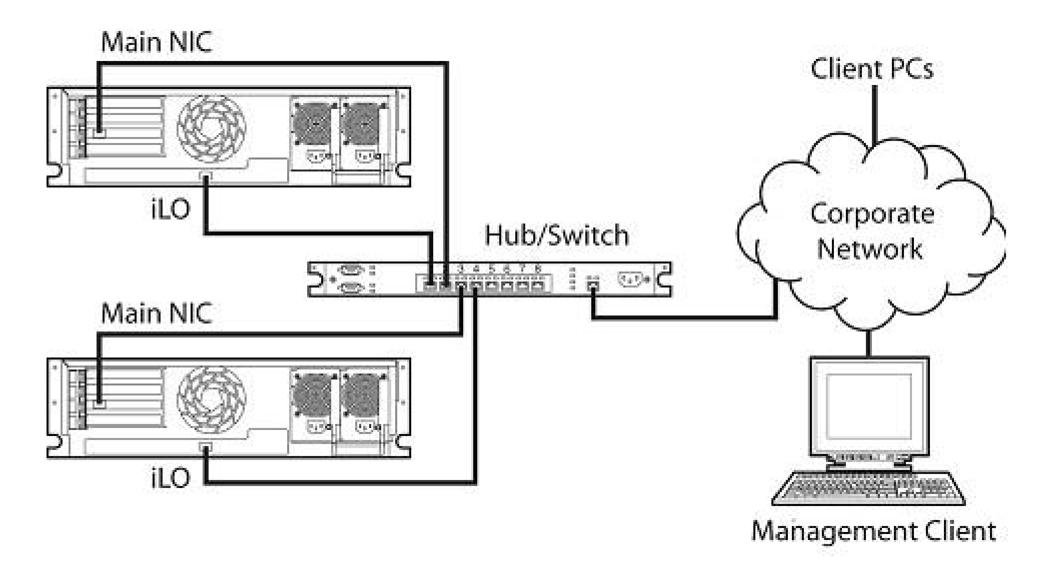
Les méthodes suivantes permettent une configuration plus avancée, impliquant plusieurs processeurs de supervision iLO 2, à l'aide de commandes de génération de script. Les scripts sont des fichiers texte écrits dans un langage de script basé sur XML appelé RIBCL. Ces scripts RIBCL permettent de configurer iLO 2 sur le réseau, pendant le déploiement initial ou à partir d'un hôte déjà déployé. Chaque méthode est décrite dans le *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

- CPQLOCFG est un utilitaire Microsoft® Windows® qui envoie des scripts RIBCL à iLO 2 via le réseau.
- HPONCFG est un utilitaire de configuration de scripts en ligne local qui s'exécute sur l'hôte et qui transmet des scripts RIBCL au iLO 2 local. Cet utilitaire existe en version Windows® et en version Linux et requiert HP iLO 2 Management Interface Driver.
- Perl est un langage de génération de scripts permettant d'envoyer des scripts RIBCL via le réseau, depuis des clients Linux vers iLO 2.

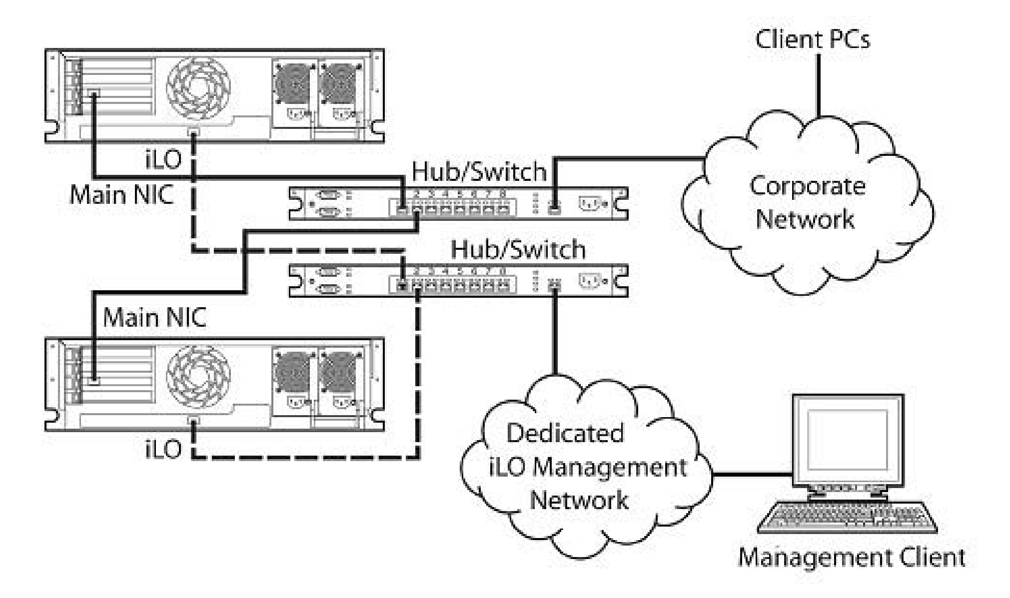
Connexion au réseau

iLO 2 se connecte au réseau de l'une des deux manières suivantes, via :

- **Corporate network** (Réseau d'entreprise) où les deux ports sont connectés au réseau d'entreprise. Dans cette configuration, les deux ports réseau du serveur (carte réseau du serveur et carte réseau iLO 2) sont connectés à un réseau d'entreprise.



- **Dedicated management network** (Réseau de supervision dédié) où le port de iLO 2 se situe sur un réseau séparé.



Configuration de l'adresse IP

Cette étape n'est nécessaire que si vous utilisez une adresse IP statique. Lorsque vous utilisez un adressage IP dynamique, votre serveur DHCP affecte une adresse IP à iLO 2 automatiquement. HP vous recommande l'utilisation d'un DNS ou d'un DHCP avec iLO 2 afin de simplifier l'installation.

Pour configurer une adresse IP statique, utilisez l'utilitaire iLO 2 RBSU en procédant comme suit afin de désactiver le DNS et le DHCP, et de configurer l'adresse IP et le masque de sous-réseau :

1. Redémarrez le serveur ou mettez-le sous tension.
2. Appuyez sur la touche **F8** lorsque vous y êtes invité pendant l'auto-test de mise sous tension (POST). L'utilitaire iLO 2 RBSU est exécuté.
3. Sélectionnez **Network**>**DNS/DHCP** (Réseau>DNS/DHCP), appuyez sur la touche **Entrée**, puis sélectionnez **DHCP Enable** (Activation de DHCP). Appuyez sur la barre d'espacement pour désactiver DHCP. Vérifiez que l'option DHCP Enable (Activation de DHCP) est désactivée et enregistrez les modifications.
4. Sélectionnez **Network**>**NIC**>**TCP/IP** (Réseau>Carte réseau>TCP/IP), appuyez sur la touche **Entrée**, puis renseignez les champs IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau) et Gateway IP Address (Adresse IP passerelle).
5. Enregistrez les modifications.
6. Quittez iLO 2 RBSU. Les modifications s'appliquent dès que vous quittez iLO 2 RBSU.

Première connexion à iLO 2

iLO 2 est configuré avec un nom d'utilisateur, un mot de passe et un nom DNS par défaut. Les informations utilisateur par défaut se trouvent sur l'étiquette iLO 2 Network Settings (Paramètres réseau iLO 2) apposée sur le serveur contenant le processeur de supervision iLO 2. Utilisez ces valeurs pour accéder à iLO 2 depuis un client réseau distant à l'aide d'un navigateur Web standard.

Pour des raisons de sécurité, HP vous recommande de modifier les paramètres par défaut après le premier accès à iLO 2.

Les valeurs par défaut sont :

- Nom d'utilisateur : Administrator
- Mot de passe : chaîne alphanumérique aléatoire de 8 caractères
- Nom DNS : *ILOXXXXXXXXXXXX*, où la série de lettres *X* correspond au numéro de série du serveur

REMARQUE : les noms d'utilisateur et les mots de passe respectent la casse.

Si vous entrez un nom utilisateur ou un mot de passe incorrect ou qu'une tentative de connexion échoue, iLO 2 vous impose un délai de sécurité. Pour plus d'informations concernant la sécurité de la connexion, reportez-vous à la section « Sécurité de la connexion » (Sécurité de la connexion à la page 44).

Configuration des comptes utilisateur

La carte iLO 2 est préconfigurée avec des valeurs par défaut, notamment un compte utilisateur et un mot de passe par défaut. Pour des raisons de sécurité, HP vous recommande de modifier les paramètres par défaut après le premier accès à iLO 2. Ces modifications peuvent être effectuées à l'aide de n'importe quelle interface utilisateur de iLO 2. Les procédures concernant l'utilitaire RBSU et le navigateur sont expliquées dans ce manuel de l'utilisateur. D'autres options, y compris l'option SMASH CLP (CLP SMASH) et les méthodes de génération de scripts, sont décrites dans le *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Si elle est connectée à un réseau qui utilise DNS ou DHCP, vous pouvez vous servir de la carte iLO 2 immédiatement sans changer aucun paramètre.

Installation de iLO 2 à l'aide de iLO 2 RBSU

HP vous recommande d'utiliser iLO 2 RBSU pour la configuration initiale de la carte iLO 2 et des paramètres réseau associés dans les environnements n'utilisant pas DHCP, DNS ou WINS. RBSU fournit les outils de base permettant de configurer les comptes utilisateur et les paramètres permettant d'accéder à iLO 2 sur le réseau.

Vous pouvez utiliser l'utilitaire RBSU pour configurer les paramètres réseau, les paramètres d'annuaire, les paramètres généraux, ainsi que les comptes utilisateur. iLO 2 RBSU ne doit pas être utilisé dans en continu. RBSU est disponible à chaque initialisation du serveur et peut être exécuté à distance à l'aide de la console distante iLO 2.

Vous pouvez désactiver l'utilitaire iLO 2 RBSU dans les préférences Global Settings (Paramètres généraux). Cela évite toute reconfiguration à partir de l'hôte, sauf si le commutateur de neutralisation de la sécurité iLO 2 est activé.

Pour exécuter iLO 2 RBSU en vue de la configuration de comptes locaux :

1. Redémarrez le serveur ou mettez-le sous tension.
2. Appuyez sur la touche **F8** lorsque vous y êtes invité pendant l'auto-test de mise sous tension (POST). L'utilitaire iLO 2 RBSU est exécuté.
3. Si le système vous le demande, entrez un nom d'utilisateur et un mot de passe iLO 2 valides avec les privilèges iLO 2 appropriés (**Administer User Accounts>Configure iLO 2 Settings** [Administrer comptes utilisateur>Configurer paramètres iLO 2]). Les informations par défaut relatives aux comptes se trouvent sur l'étiquette iLO 2 Default Network Settings (Paramètres réseau par défaut iLO 2) apposée sur le serveur contenant le processeur de supervision iLO 2. Si la carte iLO 2 n'a pas été configurée pour se connecter à RBSU, aucune invite ne s'affiche.
4. Apportez les modifications requises à la configuration de la carte iLO 2 et enregistrez-les.
5. Quittez iLO 2 RBSU.

Installation de iLO 2 à l'aide de l'option basée sur le navigateur

Utilisez la méthode d'installation basée sur le navigateur si vous pouvez vous connecter à iLO 2 sur le réseau à l'aide d'un navigateur. Cette méthode permet également de reconfigurer une carte iLO 2 déjà configurée.

Accédez à iLO 2 à partir d'un client réseau distant à l'aide d'un navigateur pris en charge et indiquez le mot de passe, le nom utilisateur et le nom DNS par défaut. Les informations relatives au compte et au nom DNS par défaut figurent sur l'étiquette iLO 2 Network Settings (Paramètres réseau iLO 2) apposée sur le serveur contenant le processeur de supervision iLO 2.

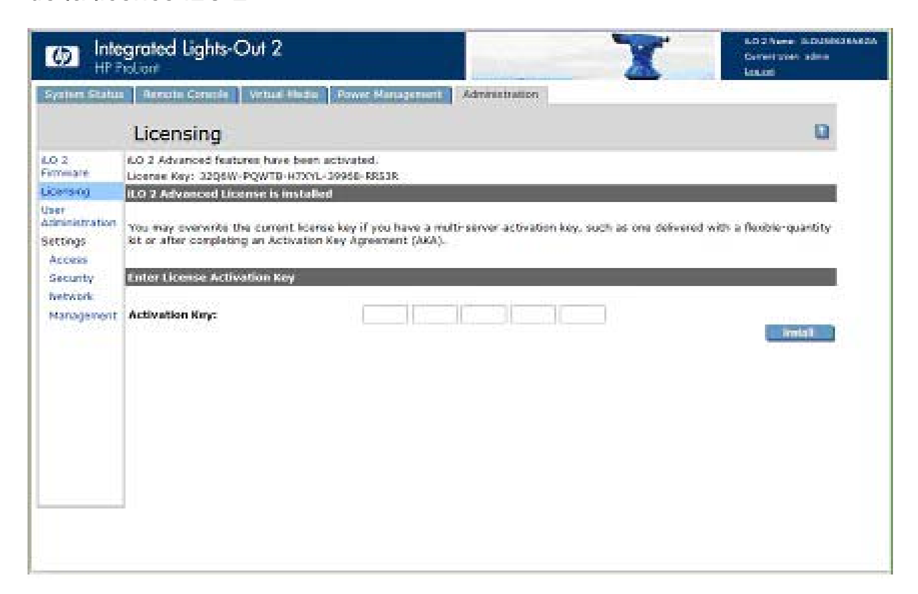
Une fois que vous avez réussi à vous connecter à iLO 2, vous pouvez modifier les valeurs par défaut des comptes utilisateur locaux en sélectionnant User Administration (Administration des utilisateurs) dans l'onglet iLO 2 Administration (Administration de iLO 2).

Activation des fonctions sous licence de iLO 2 à l'aide d'un navigateur

La page Licensing (Licence) permet de visualiser l'état de la licence en cours et de saisir la clé pour activer les fonctions sous licence de iLO 2. La version de iLO 2 et les informations sur la licence en cours sont affichées dans cette section. Si une licence est installée (y compris une licence d'évaluation),

son numéro est affiché. Pour plus d'informations concernant les options de licence iLO 2, reportez-vous à la section « Licence » (Licence à la page 21).

1. Connectez-vous à iLO 2 via un navigateur pris en charge.
2. Cliquez sur **Administration>Licensing** (Administration>Licence) pour afficher l'écran d'activation de la licence iLO 2.



3. Entrez la clé de licence. Pour passer d'un champ à un autre, utilisez la touche **Tabulation** ou cliquez dans un champ. Au fur et à mesure de la saisie dans le champ Activation Key (Clé d'activation), le curseur se déplace automatiquement. Cliquez sur **Licensing** (Licence) pour effacer les champs et recharger la page.
4. Cliquez sur **Install** (Installer). La confirmation CLUF apparaît. Les informations CLUF sont disponibles sur le site Web HP (http://www.hp.com/servers/lights-out) et dans le kit de licence.
5. Cliquez sur **OK**.

Les fonctions avancées de iLO 2 sont maintenant activées.

Installation des drivers du périphérique iLO 2

iLO 2 Management Interface Driver permet à des logiciels du système, tels que les agents SNMP Insight et le service Terminal Services Pass-Through (Passthrough des services Terminal), de communiquer avec iLO 2.

Les drivers requis pour la prise en charge de iLO 2 font partie du PSP fourni sur les CD SmartStart et Management, ou sur le site Web HP (http://www.hp.com/servers/lights-out).

Vous pouvez télécharger tous les drivers de prise en charge pour votre serveur et iLO 2 à partir du site Web HP (http://www.hp.com/servers/lights-out).

Pour ce faire :

1. Cliquez sur le graphique iLO 2.
2. Sélectionnez **Software and Drivers** (Logiciels et drivers).

Prise en charge des drivers de périphérique Microsoft

Les drivers de périphérique prenant en charge les fonctions iLO 2 sont inclus dans le PSP disponible sur le site Web HP (http://www.hp.com/support) ou sur le CD SmartStart. Avant d'installer les drivers Windows®, procurez-vous la documentation Windows® et le dernier Service Pack disponible pour Windows®.

Fichiers pré-requis pour iLO 2 :

- CPQCIDRV.SYS permet de prendre en charge iLO 2 Management Interface Driver.
- CPQASM2.SYS, SYSMGMT.SYS et SYSDOWN.SYS permettent de prendre en charge le driver de contrôleur iLO 2 Advanced Server Management.

Le PSP (ProLiant Support Pack) pour les produits Microsoft® Windows® comprend un programme d'installation qui analyse la configuration système requise et installe tous les drivers. Le PSP est disponible sur le site Web HP (http://www.hp.com/support) ou sur le CD SmartStart.

Pour installer les drivers présents dans le PSP :

1. Téléchargez le PSP à partir du site Web HP (http://www.hp.com/support).
2. Lancez le fichier SETUP.EXE téléchargé et suivez les instructions d'installation.

Pour plus d'informations sur l'installation du PSP, lisez le fichier texte inclus dans le téléchargement.

Prise en charge des drivers de périphérique Linux

Vous pouvez télécharger les fichiers LSP contenant le driver iLO 2, les agents dits « foundation agents » et les agents d'état sur le site Web HP (http://www.hp.com/support). Les instructions sur l'installation ou la mise à jour du driver iLO 2 sont disponibles sur le site Web. Les agents de supervision HP pour Linux sont les suivants :

- Le progiciel ASM (hp-snmp-agents), qui regroupe le driver d'état, l'afficheur IML, les « foundation agents », l'agent d'état et l'agent d'équipement standard en une solution unique.
- Le progiciel RSM (hp-iLO), qui combine le driver RIB, le démon de rack, l'agent RIB et l'agent de rack en une seule solution.

Pour charger les progiciels contenant les drivers d'état et les drivers iLO 2, utilisez les commandes suivantes :

```
rpm -ivh hp-snmp-agents-d.vv.v-pp.Linux_version.i386.rpm
```

```
rpm -ivh hp-iLO-d.vv.v-pp.Linux_version.i386.rpm
```

où *d* correspond à la version et au numéro de distribution Linux et

vv.v-pp au numéro de version.

Pour plus d'informations, consultez le site Web Software and Drivers (Logiciels et drivers) (http://www.hp.com/support).

Pour supprimer les drivers d'état et les drivers iLO 2, utilisez les commandes suivantes :

```
rpm -e hp-snmp-agents
```

```
rpm -e hp-iLO
```

Pour plus d'informations, consultez le site Web Software and Drivers (Logiciels et drivers) (http://www.hp.com/support).

Prise en charge des drivers de périphérique Novell NetWare

Les drivers de périphérique nécessaires à la prise en charge d'iLO 2 sont inclus dans le PSP disponible sur le CD SmartStart ou sur le site Web HP (http://www.hp.com/support). Le PSP (ProLiant Support Pack) pour Novell NetWare comprend un programme d'installation qui analyse les conditions requises pour le système et installe tous les drivers.

iLO 2 requiert les fichiers suivants :

- Le fichier CPQHLTH.NLM fournit le driver d'état (Health Driver) pour Novell NetWare.
- Le fichier CPQCI.NLM assure la prise en charge de iLO 2 Management Interface Driver.

Lors de la mise à jour des drivers iLO 2, vérifiez que iLO 2 utilise la dernière version du microprogramme. Téléchargez la dernière version en tant que Smart Component à partir du site Web HP (http://www.hp.com/servers/lights-out).

Pour installer les drivers, téléchargez le PSP sur un serveur NetWare à partir du site Web HP (http://www.hp.com/support). Après avoir téléchargé le PSP, suivez les instructions sur l'installation des composants Novell NetWare pour terminer l'installation. Pour plus d'informations sur l'installation du PSP, lisez le fichier texte inclus dans le téléchargement.

Lorsque vous utilisez Novell NetWare 6.X, vous devez utiliser le driver vidéo ATI ES1000 fourni par le système d'exploitation pour obtenir des résultats optimaux.

3 Configuration de iLO 2

Cette section traite des rubriques suivantes :

Présentation de la configuration de iLO 2

En règle générale, la configuration de iLO 2 est effectuée par des administrateurs ou des utilisateurs avancés qui doivent gérer des utilisateurs et configurer les paramètres globaux et de réseau. Pour configurer iLO 2, utilisez l'interface utilisateur iLO 2 basée sur le navigateur ou des outils de script tels que CPQLOCFG et HPONCFG (décrits dans le *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*).

L'onglet Administration iLO 2 permet de configurer et de gérer les paramètres utilisateur, le système d'alerte SNMP (via l'intégration avec HP SIM), les paramètres de sécurité, les octrois de licence, l'administration des certificats, les paramètres d'annuaire ainsi que les paramètres de l'environnement réseau. L'onglet Administration inclut les options de menu suivantes :

- iLO 2 Firmware (Microprogramme iLO 2) (Mise à jour du microprogramme iLO 2 à la page 18)
- Licensing (Licence) (Licence à la page 21)
- User Administration (Administration des utilisateurs) (Administration des utilisateurs à la page 24)
- Settings (Paramètres)
  - Access (Accès) (Configuration de l'accès à iLO 2 à la page 29)
  - Security (Sécurité) (Sécurité à la page 40)
  - Network (Réseau) (Réseau à la page 63)
  - Management (Supervision) (Paramètres SNMP/Insight Manager à la page 70)

Mise à jour du microprogramme iLO 2

Les mises à jour du microprogramme permettent d'améliorer le fonctionnement de iLO 2. Vous trouverez la dernière version du microprogramme sur le site Web HP (http://www.hp.com/servers/lights-out).

Choisissez votre produit iLO 2, puis sélectionnez **Software & Drivers** (Logiciels et drivers). Sélectionnez votre produit iLO 2 et le système d'exploitation dans la page qui s'affiche, puis cliquez sur **Locate Software** (Localiser logiciel). Vous pouvez également rechercher votre logiciel iLO 2 à l'aide des options **Operating System and Category** (Système d'exploitation et catégorie).

Vous devez disposer du privilège de configuration d'iLO 2 (configurer les paramètres d'un périphérique local) pour pouvoir mettre à jour le microprogramme, à moins que vous n'activiez le commutateur de neutralisation de la sécurité (Administration du commutateur de neutralisation de la sécurité iLO 2 à la page 42). Dans ce cas, tout utilisateur iLO 2 peut mettre à jour le microprogramme. Vous devez exécuter les mises à jour du microprogramme en tant qu'administrateur ou à partir du contexte racine du système d'exploitation du système hôte.

Pour mettre à jour iLO 2, sélectionnez l'une des méthodes suivantes :

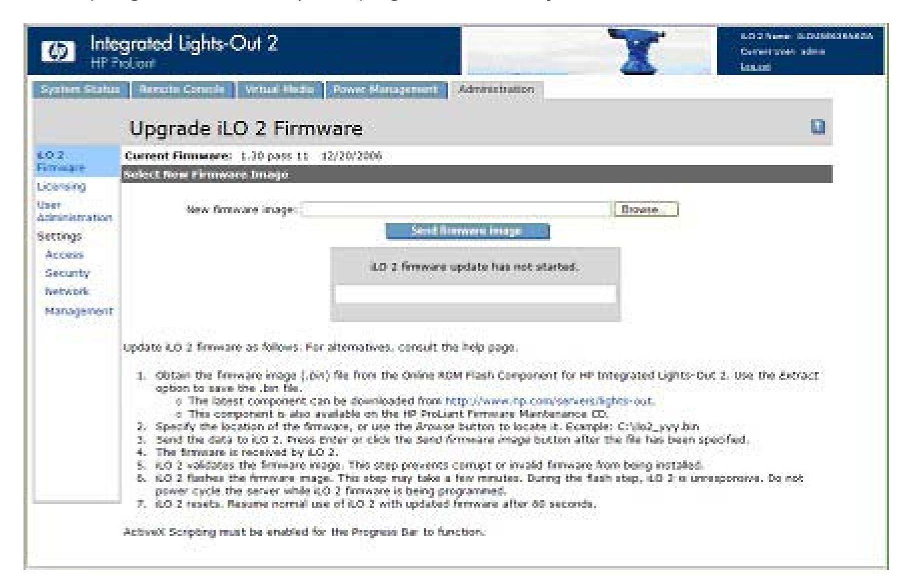
- Online firmware update (Mise à jour du microprogramme en ligne). Téléchargez le système d'exploitation approprié et exécutez-le en tant qu'administrateur ou à partir du contexte racine du système d'exploitation. Le logiciel de mise à jour du microprogramme en ligne s'exécute à partir du système d'exploitation du système hôte. Il met à jour le microprogramme de iLO 2 sans vous obliger à vous connecter à iLO 2.
- Offline firmware update for SmartStart maintenance (Mise à jour du microprogramme hors ligne pour la maintenance de SmartStart). Téléchargez le fichier image du microprogramme iLO 2 à installer et reportez-vous à la section « Mise à jour de iLO 2 à l'aide d'un navigateur » (Mise à jour de iLO 2 à l'aide d'un navigateur à la page 19).
- Firmware Maintenance CD-ROM (CD-ROM de maintenance du microprogramme). Téléchargez le composant afin de créer un CD-ROM exécutable contenant les mises à jour de plusieurs microprogrammes tels que les serveurs et les options ProLiant.
- Scripting with CPQLOCFG (Génération de scripts avec CPQLOCFG). Téléchargez le composant CPQLOCFG afin d'obtenir l'utilitaire de génération de scripts basé sur réseau, CPQLOCFG. CPQLOCFG permet d'utiliser des scripts RIBCL permettant l'exécution de mises à jour de microprogrammes, la configuration de iLO 2 et l'exécution par lots d'opérations pour iLO 2, et ce de façon sécurisée via le réseau. Pour les utilisateurs de Linux, vous devriez consulter le document HP Lights-Out XML PERL Scripting Samples for Linux (Exemples de scripts PERL et XML pour les périphériques HP Lights-Out pour Linux).
- Scripting with HPONCFG (Génération de scripts avec HPONCFG). Téléchargez le composant HPONCFG afin d'obtenir l'utilitaire de génération de scripts basé sur l'hôte, HPONCFG. Cette utilitaire permet d'utiliser des scripts RIBCL permettant l'exécution de mises à jour de microprogrammes, la configuration du processeur Lights-Out et l'exécution par lots d'opérations pour ce processeur, en tant qu'administrateur ou à partir du contexte racine des systèmes d'exploitation des systèmes hôtes pris en charge.
- HP Directories Support for Management Processors (Prise en charge des annuaires HP pour processeurs de supervision). Téléchargez l'exécutable HP Directories Support for Management Processors (Prise en charge des annuaires HP pour processeur de supervision) afin d'obtenir les composants de prise en charge d'annuaire. L'un de ses composants, HPLOMIG, peut être utilisé pour localiser les processeurs iLO, iLO 2, RILOE et RILOE II et mettre à jour leur microprogramme. Il n'est pas nécessaire d'utiliser la fonction d'intégration d'annuaire pour bénéficier de cette fonctionnalité.

Mise à jour de iLO 2 à l'aide d'un navigateur

À l'aide d'un navigateur pris en charge, vous pouvez terminer la mise à jour du microprogramme à partir de tout client réseau. Vous devez disposer du privilège adéquat pour mettre à jour le microprogramme iLO 2. Le microprogramme le plus récent pour iLO 2 est disponible sur le site Web HP (http://www.hp.com/servers/lights-out).

Pour mettre à jour le microprogramme iLO 2 à l'aide d'un navigateur, procédez comme suit :

1. Connectez-vous à la carte iLO 2 en utilisant un compte doté du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2).
2. Cliquez sur **Administration>Upgrade iLO 2 Firmware** (Administration>Mettre à niveau le microprogramme iLO 2). La page de mise à jour s'affiche.



3. Entrez le nom de fichier dans le champ New firmware image (Image du nouveau microprogramme) ou recherchez manuellement le fichier en cliquant sur Browse (Parcourir).
4. Cliquez sur **Send firmware image** (Envoyer image du microprogramme). La mise à jour du microprogramme prend quelques minutes. Une barre affiche l'état d'avancement de la mise à niveau.

N'interrompez pas la mise à jour du microprogramme iLO 2. Le système iLO 2 se réinitialise automatiquement à la fin de la mise à jour réussie du microprogramme. Cette réinitialisation n'affecte pas le système d'exploitation hôte ni le serveur.

Lorsque la mise à jour du microprogramme est interrompue ou échoue, faites immédiatement une nouvelle tentative. Ne réinitialisez pas le système iLO 2 avant d'avoir à nouveau tenter de mettre à jour le microprogramme.

Mise à jour du microprogramme à l'aide du CD de maintenance

Pour utiliser HP Smart Update Manager depuis le CD de maintenance du microprogramme :

1. Placez le CD de maintenance du microprogramme sur une clé USB à l'aide de l'utilitaire USB Key Creator Utility (Utilitaire de création de clé USB).
2. Copiez le fichier CP009768.exe dans le répertoire /compaq/swpackages sur la clé USB.
3. Suivez les instructions de HP Smart Update Manager pour mettre à jour le microprogramme.

Récupération après l'échec d'une mise à jour du microprogramme iLO 2

Pour récupérer après l'échec d'une mise à jour du microprogramme à l'aide de HP Drive Key Boot Utility (Utilitaire de lancement de la clé du lecteur HP), procédez comme suit :

1. Copiez le composant flash iLO 2 hors ligne vers votre clé d'unité USB.
2. Vérifiez que le commutateur de neutralisation de la sécurité de iLO 2 est désactivé.
3. Lancez la clé du lecteur USB contenant le composant de réécriture de iLO 2.

   Pour télécharger l'utilitaire HP Drive Key Boot Utility et obtenir des informations concernant la procédure de création d'une clé USB de démarrage, reportez-vous au site Web HP (http://www.hp.com/go/support).
4. Dans l'écran qui s'affiche, basculez vers la console de texte en appuyant sur les touches **Ctrl+Alt+F1**.
5. Basculez vers le répertoire dans lequel le composant de réécriture est stocké en saisissant `cd /mnt/usb/components/` à l'invite #.
6. Supprimez le driver HP Lights-Out chargé en saisissant les commandes suivantes :

   `/etc/init.d/hp-snmp-agents stop`

   `/etc/init.d/hp-ilo stop`

   ou

   `/etc/init.d/hpasm stop`
7. Exécutez le composant en utilisant l'option --direct. Par exemple :

   `./CP00xxxx.scexe --direct`
8. Saisissez **y** à l'invite Continue (y/N)? (Continuer [o/N] ?).
9. Une fois la programmation terminée, activez le commutateur de neutralisation de la sécurité et redémarrez le serveur.

Mise à jour descendante du microprogramme iLO 2

Si vous effectuez une mise à jour descendante du microprogramme iLO 2, vous devez supprimer l'applet 1.3.0.19 de iLO 2 Remote Console ActiveX 1.30 de votre navigateur client Internet Explorer. Pour supprimer l'applet :

1. Lancez Internet Explorer.
2. Sélectionnez **Outils>Options Internet>Paramètres>Afficher les objets**.
3. Pour supprimer 1.30.19, cliquez avec le bouton droit de la souris sur **iLO2 Remote console 1.3.0.18** (Console distante iLO 2 1.3.0.18).

Licence

Les licences de pack HP iLO Advanced et HP iLO Advanced pour BladeSystem permettent d'activer des fonctions iLO 2 facultatives non fournies avec un système sans licence. Pour plus d'informations, reportez-vous au site Web HP.

Si vous achetez le pack iLO Advanced ou iLO Advanced pour BladeSystem avec la suite logicielle Insight Control ou le pack iLO Power Management, HP fournit l'assistance technique et le service de

mise à jour. Pour plus d'informations, reportez-vous à la section « Informations concernant l'assistance » (Informations concernant l'assistance à la page 245).

Si vous achetez le pack iLO Advanced ou iLO Advanced pour BladeSystem pour une activation ponctuelle des fonctions sous licence, vous devrez acheter les mises à jour fonctionnelles ultérieures. Pour plus d'informations, reportez-vous à la section « Informations concernant l'assistance » (Informations concernant l'assistance à la page 245).

Une licence de pack iLO Advanced ou iLO Advanced pour BladeSystem est requise pour chacun des serveurs sur lequel le produit est installé et utilisé. Les licences ne peuvent pas être transférées. Il est impossible d'utiliser une licence iLO Advanced pour BladeSystem sur un serveur HP ProLiant ML/DL. Pour plus d'informations, reportez-vous au CLUF.

Sans frais supplémentaires, HP continuera d'assurer la maintenance des versions par le biais de patch et fournira les améliorations des fonctionnalités pour iLO Standard et iLO Standard Blade Edition.

Sur le site Web HP, vous pouvez télécharger une clé de licence d'évaluation valable pendant 60 jours. La licence d'évaluation s'active et permet d'accéder aux fonctions de iLO 2 Advanced. Sur chaque iLO 2, vous ne pouvez installer qu'une seule licence d'évaluation. Une fois la période d'évaluation terminée, les fonctions de iLO 2 sont inactives.

Les versions suivantes de iLO2 sont disponibles :

REMARQUE : les fonctions comportant un astérisque (*) ne sont pas prises en charge par tous les systèmes.

Élément	iLO 2 Advanced	iLO 2 Advanced pour BladeSystem	iLO 2 Standard	iLO 2 Standard Blade Edition
Commande d'alimentation virtuelle et de réinitialisation	√	√	√	√
Accès à la console du serveur par le biais d'un test POST	√	√	√	√
Console texte après le POST	√	√	—	—
Journaux d'événements	√	√	√	√
État du système* et configuration	√	√	√	√
UID	√	√	√	√
CPL standard SMASH DTMF	√	√	√	√
Fonction de génération de scripts RIBCL/XML	√	√	√	√
Génération de scripts WS-Management	√	√	√	√
Accès au navigateur	√	√	√	√
Accès SSH	√	√	√	√
Shared network port (Port réseau partagé)	√	—	√	—
Accès série	√	√	√	√

Élément	iLO 2 Advanced	iLO 2 Advanced pour BladeSystem	iLO 2 Standard	iLO 2 Standard Blade Edition
Console série distante	√	√	√	√
Console distante intégrée	√	√	—	√
Remote console (Console distante)	√	√	—	√
Applet Virtual Media	√	√	—	√
Prise en charge carte numérique sécurisée*	√	√	—	√
Passthrough de Terminal Services	√	√	—	√
Génération de scripts de support virtuel	√	√	—	—
Intégration d'annuaire	√	√	—	—
Rapports concernant l'alimentation*	√	√	—	—
Limitation dynamique de la puissance	√	√	—	—
Limitation de la puissance au niveau des groupes	√	√	—	—
Authentification à deux facteurs par carte à puce	√	√	—	—
Authentification unique HP SIM	√	√	—	—
Débogueur de noyau pour Windows	√	√	—	—
Retransmission console	√	√	—	—
Console distante partagée	√	√	—	—
Capture console boot/ fault	√	√	—	—
Lecteur vidéo iLO (licence requise pour la capture)	√	√	√	√

Outre la licence iLO 2 monoserveur standard, deux autres options de licence sont également disponibles :

- Le « Flexible Quantity License Kit » permet d'acheter une solution logicielle unique, une copie de la documentation et une seule clé de licence pour activer le nombre exact de licences requises.
- Le contrat Clé d'activation permet d'échelonner un achat volumineux de logiciels ProLiant Essentials et Insight Control. Ceux-ci sont en général achetés avec les nouveaux serveurs ProLiant (achetés en une seule fois).

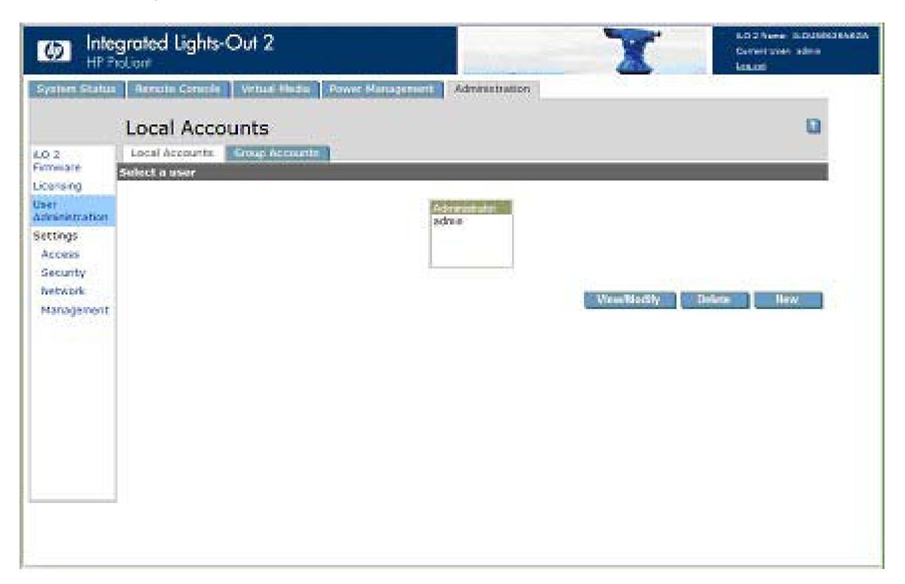
Administration des utilisateurs

iLO 2 permet de gérer les comptes utilisateur stockés localement dans la mémoire et dans les comptes de groupe de l'annuaire sécurisés iLO 2. Utilisez MMC ou ConsoleOne pour gérer les comptes utilisateur de l'annuaire.

La carte iLO 2 prend en charge jusqu'à 12 utilisateurs avec des droits d'accès et des noms de connexion personnalisables, ainsi qu'un codage avancé des mots de passe. Les privilèges permettent de contrôler les paramètres d'utilisateurs individuels. Les utilisateurs peuvent avoir des privilèges personnalisés en fonction de leurs conditions d'accès. Pour prendre en charge plus de 12 utilisateurs, vous devez disposer du pack Advanced. Celui-ci permet d'intégrer un nombre illimité de comptes utilisateur basés sur les annuaires.

Vous devez disposer du privilège Administer User Accounts (Administrer les comptes utilisateur) pour afficher les utilisateurs de iLO 2, ajouter de nouveaux utilisateurs et modifier ou supprimer des utilisateurs existants. Dans le cas contraire, vous pouvez uniquement afficher et modifier votre compte.

Pour accéder aux comptes locaux, cliquez sur **Administration>User Administration>Local Accounts** (Administration>Administration des utilisateurs>Comptes locaux).



iLO 2 Directory Accounts (Comptes d'annuaire) permet d'afficher les groupes iLO 2 et d'en modifier les paramètres. Vous devez disposer du privilège Administer Directory Groups (Administrer les groupes d'annuaires). Pour accéder aux comptes d'annuaire, cliquez sur **Administration>User Administration>Group Accounts** (Administration>Administration des utilisateurs>Comptes de groupes).



Ajout d'un nouvel utilisateur

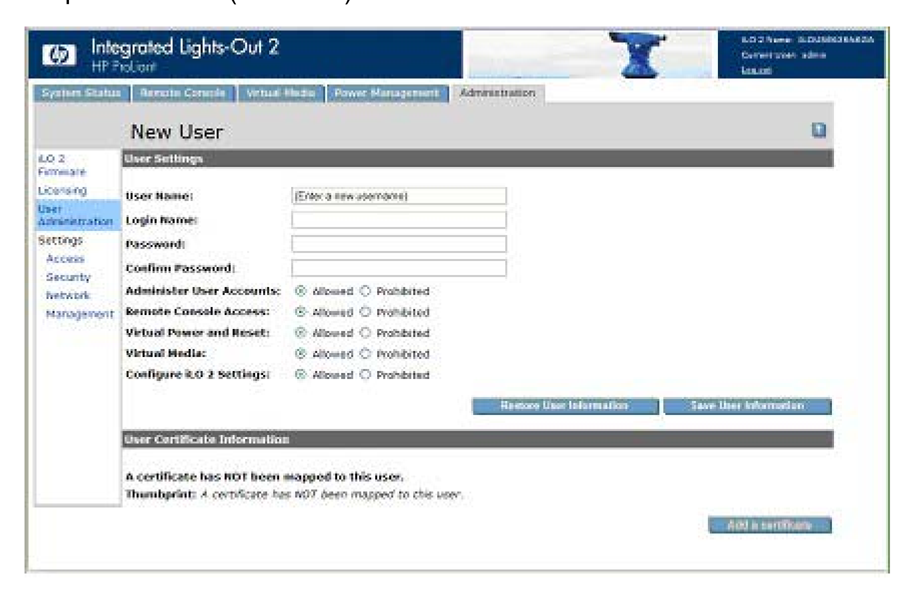
REMARQUE : seuls les utilisateurs dotés du privilège Administer User Accounts (Administrer comptes utilisateur) peuvent gérer d'autres utilisateurs sur iLO 2.

Vous pouvez attribuer des droits d'accès différents à chaque utilisateur. Chaque utilisateur peut avoir une combinaison unique de privilèges, adaptée aux tâches qu'il doit exécuter. Vous pouvez autoriser ou refuser l'accès aux fonctions critiques telles que l'accès distant, la supervision de l'utilisateur et l'alimentation virtuelle.

Pour ajouter un nouvel utilisateur à iLO 2, procédez comme suit :

1. Ouvrez une session sur la carte iLO 2 en utilisant un compte doté du privilège Administer User Accounts (Administrer comptes utilisateur).
2. Cliquez sur **Administration**.
3. Sélectionnez **User Administration>Local Accounts** (Administration des utilisateurs>Comptes locaux).

4. Cliquez sur **New** (Nouveau).



5. Renseignez les champs. Les options suivantes sont disponibles :

- User Name (Nom utilisateur) est affiché dans la liste des utilisateurs et sur la page d'accueil. Il peut être différent du nom de connexion. Sa longueur maximum est de 39 caractères. Il doit comporter des caractères imprimables.
- Login Name (Nom de connexion) est le nom à utiliser pour se connecter à iLO 2. Il ne doit pas dépasser 39 caractères. Il doit comporter uniquement des caractères imprimables.
- Les champs Password (Mot de passe) et Confirm Password (Confirmer mot de passe) permettent de définir et de confirmer le mot de passe utilisé lors de la connexion à iLO 2. La taille minimum du mot de passe se définit à la page Access Options (Options d'accès). La taille maximum d'un mot de passe est de 39 caractères. Entrez deux fois le mot de passe pour vérification.
- Administer User Accounts (Administrer comptes utilisateur) est un privilège utilisateur permettant d'ajouter, de modifier ou de supprimer les comptes utilisateur iLO 2 locaux. Il vous permet également de modifier les privilèges de tous les utilisateurs et de vous attribuer toutes les permissions. Sans ce privilège, vous pouvez uniquement afficher vos propres paramètres et modifier votre mot de passe.
- Remote Console Access (Accès console distante) est un privilège utilisateur permettant d'accéder à distance à la console distante et à la console série distante du système hôte, y compris aux contrôles vidéo, clavier et souris. Pour utiliser cette fonctionnalité, vous devez avoir accès au système distant.
- Virtual Power and Reset (Alimentation et réinitialisation virtuelles) est un privilège utilisateur permettant de mettre sous tension ou de réinitialiser la plate-forme hôte. Une de ces activités interrompt la disponibilité du système. À l'aide du bouton NMI virtuel, vous pouvez également effectuer un diagnostic du système.
- Virtual Media (Support virtuel) est un privilège utilisateur permettant d'utiliser un support virtuel sur la plate-forme hôte.
- Configure iLO 2 Settings (Configurer paramètres iLO 2) est un privilège permettant de configurer la plupart des paramètres iLO 2, y compris les paramètres de sécurité. Il vous permet de mettre à jour à distance le microprogramme iLO 2. Il ne permet pas d'administrer les comptes utilisateur. Ces paramètres changent rarement.

Après avoir configuré correctement iLO 2, la suppression de ce privilège pour tous les utilisateurs permet d'éviter une reconfiguration. Un utilisateur disposant du privilège Administer User Accounts (Administrer comptes utilisateur) peut activer ou désactiver ce privilège. Si iLO 2 RBSU est activé, vous pouvez également reconfigurer iLO 2.

- User Certificate Information (Informations sur le certificat utilisateur) associe un certificat à un utilisateur. Les certificats utilisateur sont uniquement requis pour une authentification à deux facteurs. Si aucun certificat n'est associé au compte utilisateur, le message `A certificate has NOT been mapped to this user` (Aucun certificat n'est associé à cet utilisateur) s'affiche en même temps que le bouton Add a Certificate (Ajouter un certificat). Cliquez sur ce bouton pour associer un certificat à cet utilisateur. Après avoir associé un certificat à un compte utilisateur, une empreinte à 40 chiffres du certificat s'affiche au niveau du bouton Remove this Certificate (Supprimer ce certificat). Ce dernier est utilisé pour supprimer le certificat. Si l'authentification à deux facteurs est activée, un certificat différent doit être associé à chaque utilisateur. Un utilisateur présentant un certificat lors de la connexion à iLO 2 est authentifié comme étant l'utilisateur associé à ce certificat. Cette authentification doit être activée pour permettre une authentification par certificat.

6. Une fois le profil de l'utilisateur défini, cliquez sur **Save User Information** (Enregistrer informations utilisateur) pour revenir à l'écran User Administration (Administration des utilisateurs). Pour effacer le profil saisi dans le formulaire lorsque vous entrez un nouvel utilisateur, cliquez sur le bouton **Restore User Information** (Restaurer informations utilisateur).

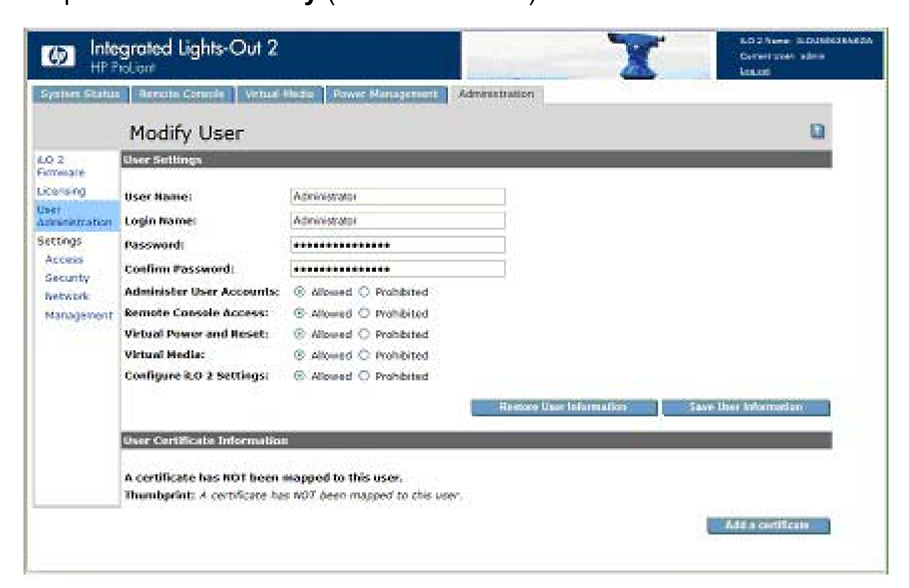
Affichage ou modification des paramètres d'un utilisateur existant

1. Ouvrez une session sur la carte iLO 2 en utilisant un compte doté du privilège Administer User Accounts (Administrer comptes utilisateur).

   Vous devez disposer du privilège Administer User Accounts (Administrer comptes utilisateur) pour gérer d'autres utilisateurs sur iLO 2. Tous les utilisateurs peuvent modifier leur propre mot de passe à l'aide de la fonction View/Modify User (Afficher/Modifier utilisateur).

2. Cliquez sur **Administration>User Administration** (Administration>Administration des utilisateurs) et sélectionnez le nom de l'utilisateur dont vous souhaitez modifier les informations.

3. Cliquez sur **View/Modify** (Afficher/Modifier).



4. Modifiez les informations utilisateur suivant les besoins.
5. Ceci fait, cliquez sur **Save User Information** (Enregistrer informations utilisateur) pour revenir à l'écran User Administration (Administration des utilisateurs). Pour restaurer les informations initiales de l'utilisateur, cliquez sur **Restore User Information** (Restaurer informations utilisateur). Toutes les modifications effectuées sur le profil sont ignorées.

Suppression d'un utilisateur

REMARQUE : seuls les utilisateurs dotés du privilège Administer User Accounts (Administrer comptes utilisateur) peuvent gérer d'autres utilisateurs sur iLO 2.

Pour supprimer les informations d'un utilisateur existant :

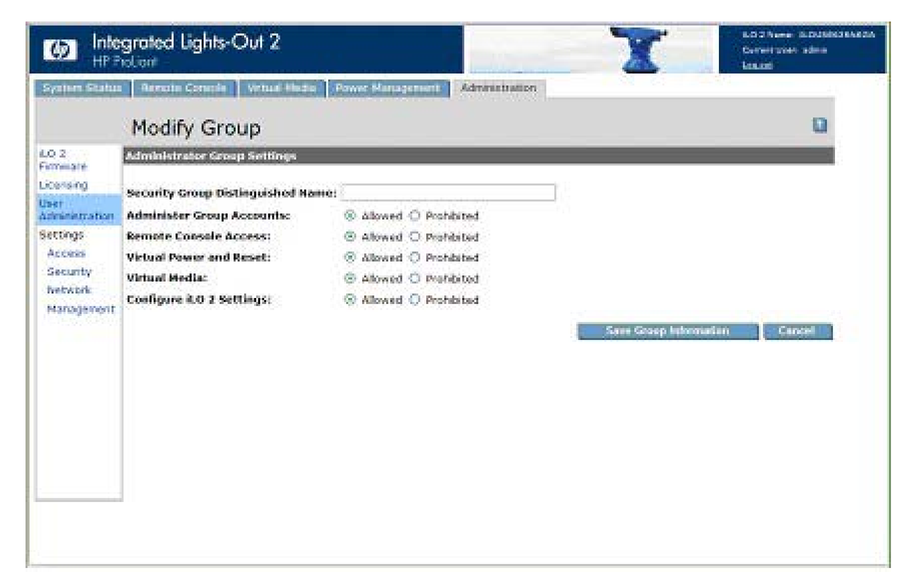
1. Ouvrez une session sur la carte iLO 2 en utilisant un compte doté du privilège Administer User Accounts (Administrer comptes utilisateur). Cliquez sur **Administration**.
2. Cliquez sur **User Administration** (Administration des utilisateurs) et sélectionnez dans la liste l'utilisateur dont vous souhaitez modifier les informations.
3. Cliquez sur **Delete User** (Supprimer utilisateur). Une fenêtre s'affiche et contient le message suivant : `Are you sure you want to delete the selected user?` (Souhaitez-vous vraiment supprimer l'utilisateur sélectionné ?). Cliquez sur **OK**.

Administration de groupe

iLO 2 permet d'afficher les groupes iLO 2 et d'en modifier les paramètres. Vous devez disposer du privilège Administer Directory Groups (Administrer les groupes d'annuaires). Pour afficher ou modifier un groupe, procédez comme suit :

1. Cliquez sur **Administration>User Administration>Group Accounts** (Administration>Administration des utilisateurs>Comptes de groupes).
2. Sélectionnez le groupe voulu et cliquez sur **View/Modify Group** (Afficher/Modifier le groupe). La page Modify Group (Modifier groupe) s'affiche.

   Cliquez sur **Cancel** (Annuler) pour revenir à la page Group Administration (Administration des groupes).



Les paramètres disponibles sont les suivants :

- Security Group Distinguished Name (Nom distinctif du groupe de sécurité) correspond au nom distinctif d'un groupe dans l'annuaire. Tous les membres de ce groupe disposent des privilèges définis pour le groupe. Le groupe défini dans Security Group Distinguished Name (Nom distinctif du groupe de sécurité) doit exister dans l'annuaire. Tous les utilisateurs devant accéder à iLO 2 doivent être membres de ce groupe. Renseignez ce champ avec un nom distinctif de l'annuaire (par exemple, CN=Group1, OU=Managed Groups, DC=domain, DC=extension).
- Administer Group Accounts (Administrer les comptes de groupes) permet aux utilisateurs appartenant à ce groupe de modifier les privilèges de n'importe quel groupe.
- Remote Console Access (Accès console distante) permet d'accéder à distance à la console distante du système hôte, y compris à la console série distante. Pour utiliser cette fonction, vous devez avoir accès au système distant.
- Virtual Power and Reset (Alimentation et réinitialisation virtuelles) permet de mettre sous tension ou de réinitialiser la plate-forme hôte. Ces activités interrompent la disponibilité du système. Si cette option est sélectionnée, vous pouvez effectuer un diagnostic du système à l'aide du bouton NMI virtuel.
- Virtual Media (Support virtuel) permet d'utiliser un support virtuel sur la plate-forme hôte.
- Configure iLO 2 Settings (Configurer paramètres iLO 2) permet de configurer la plupart des paramètres iLO 2, y compris les paramètres de sécurité. Si cette option est sélectionnée, vous pouvez mettre à jour à distance le microprogramme iLO 2. Ce paramètre n'inclut pas l'administration du compte de groupe. Ces paramètres changent rarement.

  Après avoir configuré correctement iLO 2, supprimez ce privilège pour tous les groupes afin d'éviter une reconfiguration. Les utilisateurs disposant du privilège Administer User Accounts (Administrer comptes utilisateur) peuvent l'activer et le désactiver. iLO 2 peut également être reconfiguré si l'utilitaire iLO 2 RBSU est activé.

Cliquez sur **Save Group Information** (Enregistrer informations groupe) pour enregistrer toute information mise à jour ou cliquez sur **Cancel** (Annuler) pour ignorer les modifications et revenir à la page Group Administration (Administration des groupes).

Configuration de l'accès à iLO 2

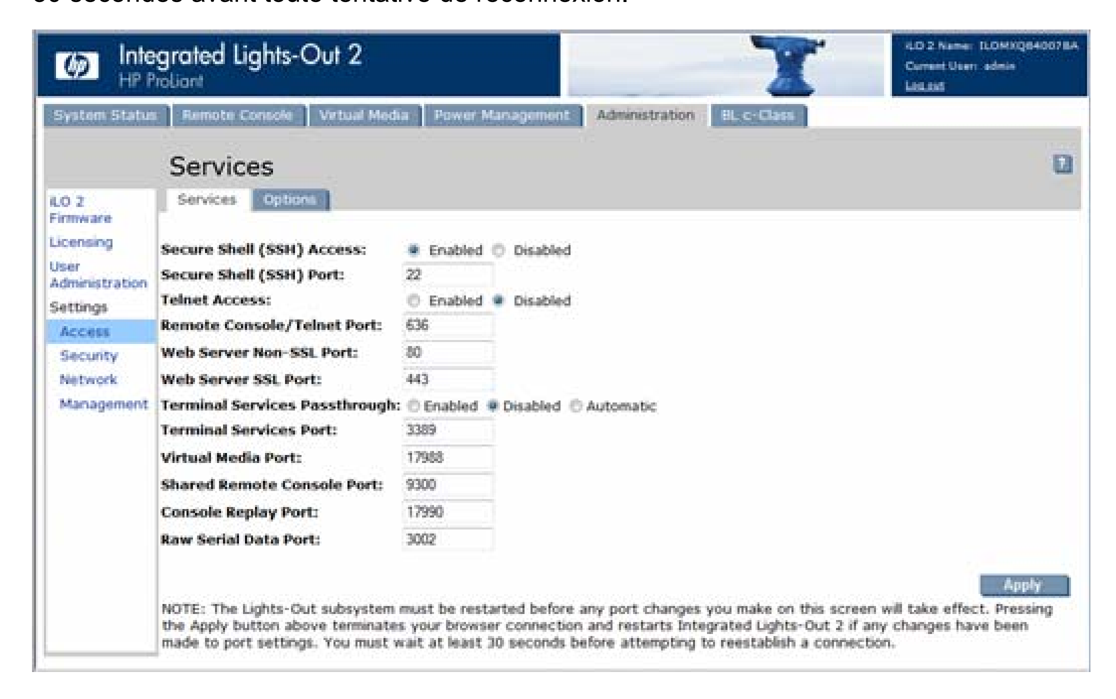
Vous pouvez configurer les services activés sur iLO 2, ainsi que l'accès à iLO 2. Pour configurer les services iLO 2 (Options des services à la page 29), cliquez sur **Administration>Access** (Administration>Accès). La page (onglet) Services s'affiche. Pour configurer l'accès à iLO 2 (Options d'accès à la page 36), cliquez sur l'onglet **Administration>Access>Options** (Administration>Accès>Options). Pour modifier les services et les options d'accès à iLO 2, vous devez disposer du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2).

Options des services

L'onglet Services permet de sélectionner les services à activer sur iLO 2, y compris SSH, SSL, la console distante, Telnet et Terminal Services. Il permet également de définir les ports de chaque option sélectionnée. Les paramètres de la page Services s'appliquent à tous les utilisateurs de iLO 2. Vous devez disposer du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2) pour modifier les paramètres de cette page.

Pour accéder aux services, cliquez sur **Administration>Access>Services** (Administration>Accès>Services). Cliquez sur **Apply** (Appliquer) pour enregistrer les informations mises à jour. Vous devez redémarrer iLO 2 pour que les modifications s'appliquent. Si vous avez effectué des modifications en vue d'activer ou de désactiver la fonctionnalité iLO 2, lorsque vous cliquez

sur **Apply** (Appliquer), votre connexion s'interrompt et iLO 2 redémarre. Vous devez patienter au moins 30 secondes avant toute tentative de reconnexion.



L'onglet Services inclut les paramètres suivants :

Paramètre	Valeur par défaut	Description
Secure Shell(SSH) Access (Accès SSH)	Activé	Ce paramètre permet de spécifier si la fonction SSH de iLO 2 est activée ou désactivée.
Secure Shell (SSH) Port (Port SSH)	22	Ce paramètre permet de configurer le port iLO 2 SSH à utiliser pour les communications SSH.
Telnet Access (Accès Telnet)	Disabled (Désactivé)	Ce paramètre permet de connecter un client Telnet à la console distante/au port Telnet, afin d'avoir accès au service CLP iLO 2. Les paramètres suivants sont valides : • Enabled (Activé) : iLO 2 autorise les clients Telnet à se connecter à la console distante/au port Telnet. Les scanners de ports réseau peuvent détecter si iLO 2 est en train d'écouter sur ce port. Les communications non codées sont autorisées entre le service CLP iLO 2 et les clients Telnet. • Disabled (Désactivé) : iLO 2 n'autorise pas les clients Telnet à se connecter à la console distante/au port Telnet. Les scanners de ports réseau n'arriveront pas à détecter si le port est ouvert sur iLO 2. Lors de l'ouverture de la console distante, iLO 2 écoute sur ce port pendant quelques secondes, mais les

Paramètre	Valeur par défaut	Description
		connexions Telnet ne sont pas acceptées. Les communications entre iLO 2 et la console distante seront toujours codées.
Remote Console/Telnet Port (Console distante/Port Telnet)	23	Ce paramètre permet de définir le port qui sera utilisé par la console distante iLO 2 pour les communications avec la console distante.
Web Server Non-SSL Port (Port non SSL du serveur Web)	80	Ce paramètre permet de définir le port qui sera utilisé par le serveur Web intégré à iLO 2 pour les communications non codées.
Web Server SSL Port (Port SSL du serveur Web)	443	Ce paramètre permet de définir le port qui sera utilisé par le serveur Web intégré à iLO 2 pour les communications codées.
Terminal Services Pass-Through (Passthrough des services Terminal)	Disabled (Désactivé)	Ce paramètre permet de contrôler la prise en charge d'une connexion via iLO 2 entre un client Microsoft® Terminal Services et un serveur Terminal Services fonctionnant sur l'hôte. Les paramètres suivants sont valides : • Automatic (Automatique) : lorsque la console distante est démarrée, le client Terminal Services est lancé. • Enabled (Activé) : la fonction Passthrough est activée et le client Terminal Services peut être directement connecté à iLO 2 sans avoir à s'identifier auprès de iLO 2. • Disabled (Désactivé) : la fonction Passthrough est désactivée.
Terminal Services Port (Port des Terminal Services)	3389	Ce paramètre permet de définir le port des services de terminal utilisé par iLO 2 pour les communications codées avec les logiciels Passthrough des services de terminal sur le serveur. Si ce port est configuré sur un port autre que celui défini par défaut, vous devez modifier manuellement le numéro de port.
Virtual Media Port (Port du support virtuel)	17988	Ce paramètre permet de définir le port de la prise en charge du support virtuel pour les communications iLO 2.
Shared Remote Console Port (Port de la console distante partagée)	9300	Ce paramètre permet de définir le port de la console distante partagée. Ce port est ouvert sur le client pour permettre à des utilisateurs supplémentaires de se connecter à la console distante, de la même manière qu'en peer-to-peer. Ce port est uniquement ouvert lorsque la console distante partagée est utilisée.

Paramètre	Valeur par défaut	Description
Console Replay Port (Port de retransmission console)	17990	Ce paramètre permet de définir le port de retransmission console. Ce port est ouvert sur le client pour activer le transfert de la mémoire tampon de capture interne vers le client pour la retransmission. Ce port est uniquement ouvert si la mémoire tampon de capture est transférée vers le client.
Raw Serial Data Port (Port de données série brutes)	3002	Ce paramètre permet de définir l'adresse du port de données série brutes. Ce port est uniquement ouvert lorsque l'utilitaire WiLODbg.exe est utilisé pour déboguer le serveur hôte à distance.

Option Passthrough des services terminal

Terminal Services est une fonctionnalité des systèmes d'exploitation Microsoft® Windows®. L'option Terminal Services Pass-Through (Passthrough des services Terminal) de iLO 2 fournit une connexion entre le serveur Terminal Services du système hôte et le client Terminal Services sur le système client. Lorsqu'elle est activée, le microprogramme iLO 2 active un connecteur, en écoutant par défaut sur le port 3389. Toutes les données envoyées par Terminal Services sur ce port sont transmises au serveur et toutes celles envoyées par le serveur sont retransmises au connecteur. Le microprogramme iLO 2 lit tout ce qui est reçu sur ce port en tant que paquet RDP. Les paquets RDP sont échangés entre le microprogramme iLO 2 et le serveur Terminal Services (RDP) via l'adresse hôte locale sur le serveur. Le service fourni facilite la communication entre iLO 2 et le serveur RDP. Ce dernier interprète le service en tant que connexion RDP externe établie. Pour plus d'informations sur le service RDP, reportez-vous à la section « Service Passthrough Windows® RDP » (Service Passthrough Windows RDP à la page 33).

Une session Terminal Services fournit une vue améliorée de la console du système hôte. Lorsque le système d'exploitation (ou le serveur ou le client Terminal Services) est indisponible, c'est la console distante traditionnelle iLO 2 qui fournit une vue de la console du système hôte. Pour plus d'informations sur la console distante et sur les clients Terminal Services, reportez-vous à la section « Console distante et clients Terminal Services » (Console distante et clients Terminal Services à la page 35).

Pour configurer l'option Terminal Services Passthrough, reportez-vous aux sections « Conditions requises pour le client Terminal Services » (Conditions requises pour le client Terminal Services à la page 33) et « Installation de l'option Terminal Services Pass-Through (Passthrough des services Terminal) » (Installation de l'option Terminal Services Passthrough (Passthrough des services Terminal) à la page 33).

Conditions requises pour le client Terminal Services

Le client Terminal Services est disponible sur des machines client Microsoft® Windows® exécutant :

- Windows Server® 2003

  Sur les serveurs Windows Server® 2003, le client Terminal Services et la connexion RDP sont intégrés. Le client fait partie du système d'exploitation et est activé à l'aide du partage des bureaux à distance. Pour activer le partage des bureaux, sélectionnez **Poste de travail>Propriétés>Utilisation à distance>Bureau à distance**. Le client Terminal Services sous Windows Server® 2003 propose des options de ligne de commande et des lancements en toute transparence à partir de l'applet de la console distante.

- Windows Server® 2008

  Sur les serveurs Windows Server® 2008, le client Terminal Services et la connexion RDP sont intégrés. Le client fait partie du système d'exploitation et est activé à l'aide du partage des bureaux à distance. Pour activer le partage des bureaux, sélectionnez **Poste de travail>Propriétés>Utilisation à distance>Bureau à distance**. Le client Terminal Services sous Windows Server® 2008 propose des options de ligne de commande et des lancements en toute transparence à partir de l'applet de la console distante.

- Windows® XP

  Sur les serveurs Windows® XP, la connexion Terminal Services et RDP est intégrée. Le client fait partie du système d'exploitation et est activé à l'aide du partage des bureaux à distance. Pour activer le partage des bureaux, sélectionnez **Démarrer>Programmes>Accessoires>Communications>Bureau à distance**. Le client Terminal Services sous Windows® XP fournit des options de ligne de commande et des lancements à partir de l'applet de la console distante.

Service Passthrough Windows RDP

Pour utiliser la fonction Passthrough de Terminal Services iLO 2, vous devez installer un service Passthrough sur le système hôte. Ce service affiche le nom du proxy iLO 2 dans la liste d'hôtes des services disponibles. Il utilise la sécurité et la fiabilité Microsoft® .NET framework. Après le démarrage du service, celui-ci interroge iLO 2 pour détecter si une connexion RDP avec le client a été établie. Si tel est le cas, le service établit une connexion TCP avec l'hôte local et commence l'échange des paquets. Le port utilisé pour communiquer avec l'hôte local se trouve à l'adresse de registre Windows® suivante :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\Wds
\rdpwd\Tds\tcp\PortNumber
```

En règle générale, ce port est le port 3389.

Installation de l'option Terminal Services Passthrough (Passthrough des services Terminal)

La section suivante explique comment installer le Passthrough de Terminal Services sur Windows Server® 2008, Windows Server® 2003 et Microsoft® Windows® XP.

- Windows Server® 2003 et Windows Server® 2008

  Les serveurs Windows® requièrent Microsoft® .NET Framework pour prendre en charge l'utilisation de Terminal Services iLO 2. Le service Passthrough de Terminal Services ainsi qu'iLO 2

Management Interface Driver pour Windows® 2008 et Windows Server® 2003 doivent être installés sur le serveur disposant d'iLO 2.

a. Installez iLO 2 Management Interface Driver.

b. Installez le service Passthrough. Pour installer le service, lancez le composant d'installation et suivez les instructions de l'assistant d'installation.

Si le service est déjà installé, vous devez relancer manuellement ou redémarrer le serveur lors de l'installation du driver.

c. Activez le client Terminal Services.

Sur Windows Server® 2003 et Windows Server® 2008, vous pouvez activer le partage des bureaux à distance en cliquant sur l'onglet **Utilisation à distance**, sous Poste de travail>Propriétés.

Si l'installation de iLO 2 est terminée et si la fonction Terminal Services Pass-Through (Passthrough de Terminal Services) est définie sur l'option automatique, le client Terminal Services s'exécute à la fin de l'installation.

- Microsoft® Windows® XP

  Sous Windows® XP, la connexion au bureau à distance est intégrée et ne requiert pas de spécifications d'installation supplémentaires.

Les erreurs survenant lors de l'installation et de l'exécution du service Passthrough sont consignées dans le journal d'événements de l'application serveur. Utilisez l'option Ajout/suppression de programmes du Panneau de configuration pour supprimer ce service.

Activation de l'option Passthrough des services Terminal

Cette fonction est désactivée par défaut et peut être activée depuis la page Administration>Access>Services (Administration>Accès>Services). Le bouton Terminal Services (Services Terminal) de la console distante est désactivé jusqu'à l'activation de la fonction Terminal Services Pass-Through (Passthrough des services Terminal).

Pour utiliser la fonction Terminal Services Pass-Through (Passthrough des services Terminal), installez la dernière version de Lights-Out Management Interface Driver, puis installez à nouveau le service Passthrough des services Terminal pour Microsoft® Windows® sur le serveur.

Lorsque l'option Terminal Services Pass-Through (Passthrough de Terminal Services) est définie sur Enabled (Activé) ou Automatic (Automatique) dans la page Administration>Access>Services (Administration>Accès>Services) et que le client Terminal Services est installé sur le client Windows® (installé par défaut sur Windows® XP), le bouton Terminal Services est activé. Lorsque ce bouton est activé, l'applet essaye de lancer Terminal Services, même si le serveur n'exécute pas de système d'exploitation Windows®.

Vous devez respecter les spécifications de la licence Microsoft® qui sont les mêmes que pour la connexion via la carte réseau du serveur. Par exemple, lorsqu'elle est définie pour un accès administrateur, la fonction Terminal Services (Services Terminal) autorise deux connexions au plus, que celles-ci soient effectuées via la carte réseau serveur, la carte iLO 2 ou les deux.

Message d'avertissement de Terminal Services

Les utilisateurs de Terminal Services (Services Terminal) travaillant sous Windows® 2003 Server peuvent être confrontés au problème suivant lorsqu'ils utilisent la fonction Terminal Services Pass-Through (Passthrough des services Terminal) de iLO 2 : lorsqu'une session Terminal Services (Services Terminal) est établie via iLO 2 et qu'une deuxième session Terminal Services (Services Terminal) est établie par un administrateur Windows® (mode Console), la première session est déconnectée.

Cependant, la première session ne reçoit de message d'avertissement indiquant la déconnexion qu'au terme d'un délai d'une minute environ. Pendant ce temps, la première session est disponible ou active. Cette situation est tout à fait normale, mais différente de celle observée lorsque deux sessions Terminal Services sont établies par des administrateurs Windows®. Dans ce cas, la première session reçoit immédiatement le message d'avertissement.

Affichage de l'option Passthrough de Terminal Services

Le microprogramme iLO 2 peut ne pas afficher avec précision l'option Passthrough de Terminal Services. L'option Passthrough de Terminal Services s'affiche comme étant active même si elle ne l'est pas sur le système d'exploitation (tel est le cas sur un système d'exploitation Linux).

Console distante et clients Terminal Services

Il est possible de recourir à une session de console distante iLO 2 pour afficher une session Terminal Services sur l'hôte, via la connexion à un réseau de supervision iLO 2. Lorsque l'applet de la console distante iLO 2 s'exécute, elle lance le client Terminal Services, basé sur la préférence utilisateur. Il est nécessaire d'installer les Machines virtuelles Sun pour exploiter pleinement cette fonctionnalité. Lorsque les Machines virtuelles Sun ne sont pas installées, la console distante ne peut pas lancer le client Terminal Services automatiquement.

Lorsque l'option Terminal Services Pass-Through (Passthrough des services Terminal) est activée et que le serveur Terminal Services est disponible, le basculement entre la console distante de iLO 2 et le client Terminal Services se fait de façon transparente, au fur et à mesure de la progression du serveur d'un environnement préalable au système d'exploitation vers un environnement sans système d'exploitation disponible, en passant par un environnement dans lequel s'exécute un système d'exploitation. La transparence de l'opération est valable tant que le client Terminal Services n'est pas lancé avant que la console distante soit disponible. Si ces fonctionnalités sont toutes deux disponibles, la console distante lance le client Terminal Services au moment opportun.

Lorsque la fonction de Passthrough de Terminal Services est utilisée avec Windows Server® 2003 et Windows Server® 2008, vous devrez patienter environ 30 secondes entre le moment où la boîte de dialogue Ctrl-Alt-Suppr disparaît et où le client Terminal Services démarre. Ce délai représente le temps nécessaire au service pour se connecter au client RDP qui s'exécute sur le serveur. Si le serveur est réamorcé à partir du client Terminal Services, l'écran Remote Console (Console distante) devient grisé ou noir pendant près d'une minute, le temps nécessaire à la carte iLO 2 pour constater que le serveur Terminal Services n'est plus disponible.

Lorsque le mode Terminal Services est défini sur Enabled (Activé) et que vous souhaitez utiliser la console distante, vous devez lancer le client Terminal Services directement à partir de son menu. Cela permet d'utiliser simultanément le client Terminal Services et la console distante.

La fonctionnalité Terminal Services peut être désactivée ou activée à tout moment. La modification de la configuration des services Terminal entraîne la réinitialisation du microprogramme iLO 2. La réinitialisation du microprogramme iLO 2 a pour effet d'interrompre toutes les connexions ouvertes établies vers iLO 2.

Lorsque le client Terminal Services est lancé à l'aide de la fonction Remonte Console (Console distante), cette dernière passe en mode veille pour éviter de consommer de la largeur de bande de l'unité centrale. Pour toutes les commandes iLO 2, la fonction Remote Console utilise toujours par défaut le port 23 de la console distante.

La carte iLO 2 effectue une seule émulation par connexion Terminal Services à la fois. La fonctionnalité Terminal Services est limitée à deux sessions simultanées.

Lorsqu'elle est en mode veille, la console distante devient active et disponible si le client Terminal Services est interrompu pour l'une des raisons suivantes :

- le client Terminal Services est fermé par l'utilisateur ;
- le système d'exploitation Windows® est arrêté ;
- le système d'exploitation Windows® se bloque.

Résolution des problèmes liés à Terminal Services

Pour résoudre les problèmes liés au Passthrough des services Terminal iLO 2, procédez comme suit :

1. Assurez-vous que le client Terminal Services est activé sur l'hôte. Pour ce faire, sélectionnez **Poste de travail>Propriétés>Utilisation à distance>Bureau à distance**.
2. Pour vérifier que la configuration Passthrough de iLO 2 est activée ou automatique, consultez les paramètres généraux iLO 2.
3. Vérifiez que vous disposez d'une licence pour le pack iLO Advanced.
4. Vérifiez que iLO 2 Management Interface Driver est installé sur l'hôte. Pour ce faire, sélectionnez **Poste de travail>Propriétés>Matériel>Gestionnaire de périphériques>Cartes multifonctions**.
5. Vérifiez que le service Passthrough de Terminal Services et iLO 2 Proxy sont installés et qu'ils fonctionnent sur l'hôte. Pour ce faire, sélectionnez **Panneau de configuration>Outils d'administration>Services** et essayez de relancer le service.
6. Vérifiez que le journal d'événements de l'application n'est pas saturé.

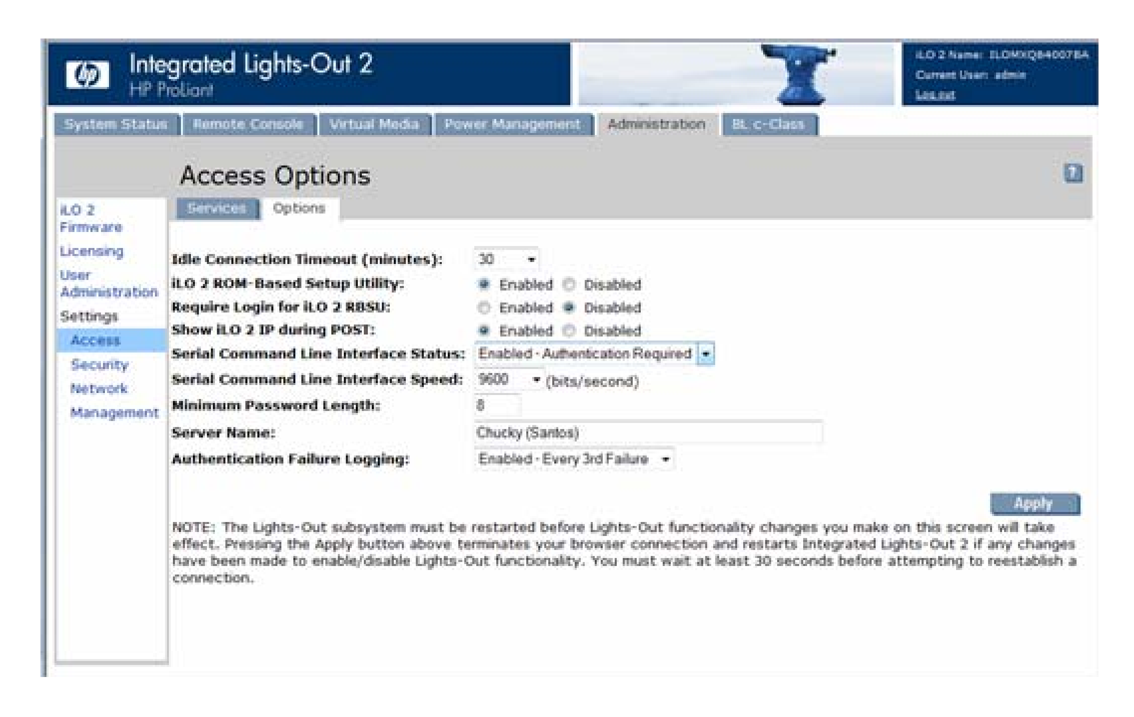
   Le service d'émulation Terminal Services peut rencontrer des problèmes de démarrage lorsque le journal d'événements de l'application du système d'exploitation est saturé. Pour afficher le journal d'événements, sélectionnez **Gestion de l'ordinateur>Outils système>Observateur d'événements>Application**.
7. Vérifiez que l'affectation du port Terminal Services est correcte.
8. Vérifiez que le client Terminal Services `mstsc.exe` se trouve dans le répertoire `\WINDOWS\SYSTEM32`.

   Si ce n'est pas le cas, définissez le Passthrough sur **Enabled** (Activé) et activez manuellement le client Terminal Services.

Options d'accès

iLO 2 permet de modifier l'accès à iLO 2, y compris le temps d'inactivité de la connexion, la fonctionnalité iLO 2, iLO 2 RBSU, les conditions de connexion, les paramètres CLI, la longueur minimale du mot de passe et le nom du serveur. Les paramètres de la page Access Options (Options d'accès) s'appliquent à tous les utilisateurs de iLO 2. Vous devez disposer du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2) pour modifier les paramètres de cette page.

Pour afficher ou modifier l'accès à iLO 2, cliquez sur **Administration>Access>Options** (Administration>Accès>Options), puis cliquez sur **Apply** (Appliquer) pour enregistrer les informations mises à jour. Vous devez redémarrer iLO 2 pour que les modifications s'appliquent. Si vous avez effectué des modifications en vue d'activer ou de désactiver la fonctionnalité iLO 2, cliquez sur **Apply** (Appliquer) pour arrêter votre connexion et redémarrer iLO 2. Vous devez patienter au moins 30 secondes avant toute tentative de reconnexion.



L'onglet Options comprend les éléments suivants :

Paramètre	Valeur par défaut	Descriptions
Idle Connection Timeout (minutes) (Délai d'inactivité de la connexion - minutes)	30 minutes	Ce paramètre spécifie l'intervalle d'inactivité de l'utilisateur (en minutes) avant que la session Web et de console distante ne soit interrompue automatiquement. Les paramètres suivants sont valides : 15, 30, 60, 120 minutes ou 0 (illimité). La valeur du délai d'attente illimité ne déconnecte pas les utilisateurs inactifs.
Lights-Out Functionality (Fonctionnalité Lights-Out)	Activé	Ce paramètre permet la connexion à iLO 2. Lorsqu'elle est désactivée, toutes les connexions à iLO 2 sont rejetées. Les capacités de réseau 10/100 et de communication de la carte iLO 2 avec les drivers du système d'exploitation seront inactivées si la fonctionnalité Lights-Out est désactivée. Le port de diagnostic de iLO 2 pour un serveur HP ProLiant BL p-Class est également désactivé. Si la fonctionnalité iLO 2 est désactivée (y compris le port de diagnostic iLO 2), vous devez utiliser le commutateur de neutralisation de la sécurité iLO 2 du serveur pour l'activer. Reportez-vous à la documentation du serveur pour localiser ce commutateur et l'activer. Mettez le serveur sous tension et utilisez iLO 2 RBSU pour définir la fonctionnalité Lights-Out sur Enabled (Activée).
iLO 2 ROM-Based Setup Utility (Utilitaire iLO 2 RBSU)	Activé	Ce paramètre active ou désactive l'utilitaire iLO 2 RBSU. Normalement, l'option ROM iLO 2 vous invite à appuyer

Paramètre	Valeur par défaut	Descriptions
		sur **F8** pour accéder à cet utilitaire, mais si iLO 2 ou l'utilitaire iLO 2 RBSU est désactivé, l'invite RBSU est contournée.
Require Login for iLO 2 RBSU (Exiger connexion pour utilitaire iLO 2 RBSU)	Disabled (Désactivé)	Ce paramètre permet d'accéder au RBSU avec ou sans les données d'authentification utilisateur. S'il est activé et que vous appuyez sur la touche **F8** lors de la séquence POST pour accéder à iLO 2 RBSU, une boîte de dialogue de connexion s'affiche.
Show iLO 2 during POST (Afficher iLO 2 pendant POST)	Disabled (Désactivé)	Ce paramètre permet d'afficher l'adresse IP du réseau iLO 2 lors de la séquence POST sur le serveur hôte.
Serial Command Line Interface Status (État de l'interface de ligne de commande série)	Enabled-Authentication Required (Activé-Authentification requise)	Ce paramètre permet de modifier le modèle de connexion de la fonction CLI via le port série. Les paramètres suivants sont valides : • Enabled-Authentication Required (Activé-Authentification requise) • Enabled—No Authentication (Activé-Aucune authentification) • Disabled (Désactivé)
Serial Command Line Interface Speed (Vitesse de l'interface de ligne de commande série)	9600	Ce paramètre permet de modifier la vitesse du port série de la fonction CLI via le port série. Les vitesses suivantes (en bits/s) conviennent : 9 600, 19 200, 38 400, 57 600 et 115 200. Pour un fonctionnement correct, la configuration du port série doit être la suivante : Pas de parité, 8 bits de données et 1 bit d'arrêt (N/8/1). La vitesse du port série définie par ce paramètre doit correspondre à celle du port série définie dans la configuration du RBSU de la ROM système.
Minimum Password Length (Longueur minimale du mot de passe)	8	Ce paramètre permet de spécifier un nombre minimum de caractères requis lorsque le mot de passe de l'utilisateur est paramétré ou modifié. La longueur des caractères peut être définie par une valeur comprise entre 0 et 39.

Paramètre	Valeur par défaut	Descriptions
Server Name (Nom du serveur)	—	Ce paramètre permet d'indiquer le nom du serveur hôte. Cette valeur est attribuée lors de l'utilisation d'agents de supervision HP ProLiant. Si aucun agent n'est utilisé et qu'un message concernant l'hôte non nommé s'affiche, utilisez ce paramètre. Lorsque les agents sont en cours d'exécution, la valeur affectée peut être remplacée. Pour forcer le rafraîchissement du navigateur, enregistrez ce paramètre et appuyez sur **F5**.
Authentication Failure Logging (Consignation des échecs d'authentification)	Enabled-Every 3rd Failure (Activé-Au troisième échec)	Ce paramètre permet de configurer les critères de consignation des authentifications ayant échoué. Tous les types de consignation sont pris en charge et fonctionnent indépendamment les uns des autres. Les paramètres suivants sont valides : • Enabled-Every Failure (Activé-Tous les échecs) : pour chaque échec de connexion, une entrée est consignée dans le journal des connexions ayant échoué. • Enabled-Every 2nd Failure (Activé-Au deuxième échec) : à la deuxième tentative de connexion ayant échoué, une entrée est consignée dans le journal. • Enabled-Every 3rd Failure (Activé-Au troisième échec) : à la troisième tentative de connexion ayant échoué, une entrée est consignée dans le journal. • Enabled-Every 5th Failure (Activé-Au cinquième échec) : à la cinquième tentative de connexion ayant échoué, une entrée est consignée dans le journal. • Disabled—(Désactivé) : aucune entrée n'est consignée dans le journal pour un échec de connexion.

Lors de la connexion à iLO 2 avec des clients Telnet ou SSH, le nombre d'invites de connexion correspond à la valeur du paramètre Authentication Failure Logging (Consignation des échecs d'authentification). Il est de 3 si ce paramètre est désactivé. Cependant, le nombre d'invites est aussi affecté par les configurations des clients SSH et Telnet. Les connexions Telnet et SSH disposent également d'un délai après un échec de connexion. Lors de ce délai, la connexion est désactivée. Aucun échec ne survient. Exemple : pour générer un journal d'échec d'authentification SSH avec une valeur par défaut, telle que Enabled-Every 3rd Failure (Activé-Au troisième échec), trois échecs consécutifs

de connexion surviennent comme suit (en considérant que le nombre d'invites de mot de passe sur le client SSH est supérieur ou égal à 3) :

1. Exécutez le client SSH et connectez-vous en utilisant un nom de connexion et un mot de passe incorrects. Vous recevrez trois invites de mot de passe. Après le troisième mot de passe incorrect, la connexion est interrompue et un premier échec de connexion est consigné. Le compteur d'échecs de connexion SSH est défini sur 1.
2. Exécutez le client SSH jusqu'à ce que vous soyez invité à vous connecter. Connectez-vous à l'aide d'un nom ou d'un mot de passe de connexion incorrect. Vous recevrez trois invites de mot de passe. Après le troisième mot de passe incorrect, la connexion est fermée et un deuxième échec de connexion est consigné. Le compteur d'échecs de connexion SSH est défini sur 2.
3. Exécutez le client SSH jusqu'à ce que vous soyez invité à vous connecter. Connectez-vous à l'aide d'un nom ou d'un mot de passe de connexion incorrect. Vous recevrez trois invites de mot de passe. Après le troisième mot de passe incorrect, la connexion est fermée et un troisième échec de connexion est consigné. Le compteur d'échecs de connexion SSH est défini sur 3.

À ce stade, le microprogramme iLO 2 consigne une entrée d'échec de connexion SSH dans le journal et définit le compteur d'échecs de connexion SSH sur 0.

Accès à la console distante et à la console série distante iLO 2

Pour plus d'informations sur les paramètres client recommandés de la console distante iLO 2, les paramètres du serveur, l'optimisation de la prise en charge de la souris et les paramètres de la console série distante, reportez-vous à la section « Console distante iLO 2 » (Console distante iLO 2 à la page 89).

Sécurité

iLO 2 permet de personnaliser les paramètres de sécurité. Pour accéder aux paramètres de sécurité iLO 2, sélectionnez **Administration>Security** (Administration>Sécurité). Les options de sécurité iLO 2 sont les suivantes :

- Administration de clé SSH (Administration de clé SSH à la page 44)
- Administration de certificat SSL (Administration des certificats SSL à la page 45)
- Authentification à deux facteurs (Authentification à deux facteurs à la page 46)
- Paramètres d'annuaire (Directory Settings (Paramètres d'annuaire) à la page 52)
- Codage iLO 2
- Authentification unique HP SIM (HP SIM single sign-on (Authentification unique HP SIM) (SSO) à la page 58)
- Verrou d'ordinateur de console distante (Remote Console Computer Lock (Verrou d'ordinateur de console distante) à la page 61)

Les options de sécurité permettent à iLO 2 de fournir les fonctions de sécurité suivantes :

- Ports TCP/IP définis par l'utilisateur
- Actions utilisateur consignées dans le journal des événements de la carte iLO 2
- Délais progressifs des échecs de connexion
- Prise en charge des certificats signés X.509 CA
- Prise en charge de la sécurisation RBSU

- Communication codée à l'aide de :
  - Administration de clé SSH
  - Administration des certificats SSL
- Prise en charge de services d'annuaire basés sur LDAP facultatifs

Certaines de ces options sont sous licence. Pour consulter la liste des options disponibles, reportez-vous à la section « Licence » (Licence à la page 21).

Consignes générales de sécurité

Cette section présente les principes généraux applicables à la carte iLO 2 en matière de sécurité :

- Pour une sécurité maximale, installez la carte iLO 2 sur un réseau de supervision distinct.
- La carte iLO 2 ne doit pas être directement connectée à Internet.
- Utilisez un navigateur possédant une capacité de codage de 128 bits.

Principes relatifs aux mots de passe

La liste suivante indique les principes recommandés pour le choix des mots de passe.

- Ne jamais conserver de trace écrite ou enregistrée des mots de passe.
- Ne jamais partager les mots de passe avec d'autres utilisateurs.
- Ne pas utiliser des mots courants du dictionnaire ou des mots faciles à deviner tels que le nom de votre entreprise, le nom d'un produit, le nom de l'utilisateur ou son identifiant.
- Les mots de passe doivent satisfaire au moins trois des quatre caractéristiques suivantes :
  - au moins un caractère numérique ;
  - au moins un caractère spécial ;
  - au moins un caractère minuscule ;
  - au moins un caractère majuscule.

Les mots de passe délivrés pour un ID utilisateur temporaire, une réinitialisation du mot de passe ou un ID utilisateur verrouillé doivent également respecter ces normes. Chaque mot de passe doit avoir une longueur comprise entre 0 et 39 caractères. La longueur minimale par défaut est de 8 caractères. HP vous déconseille de définir la longueur minimale du mot de passe sur moins de 8 caractères, sauf si vous disposez d'un réseau de supervision sécurisé physiquement qui ne s'étend pas au-delà du centre de données sécurisé.

Sécurisation de RBSU

iLO 2 RBSU permet d'afficher et de modifier la configuration iLO 2. Vous pouvez configurer les paramètres d'accès à RBSU à l'aide de l'utilitaire RBSU, d'un navigateur Web (Options d'accès

à la page 36), de scripts RIBCL ou du commutateur de neutralisation de la sécurité iLO 2. RBSU comporte trois niveaux de sécurité :

- RBSU Login Not Required (Connexion RBSU non requise) (niveau par défaut)

  Les utilisateurs qui peuvent accéder à l'hôte pendant l'auto-test de mise sous tension (POST) peuvent accéder à l'utilitaire iLO 2 RBSU pour afficher et modifier les paramètres de configuration. Ce paramètre est valide si l'accès à l'hôte est contrôlé.

- RBSU Login Required (Connexion RBSU requise) (niveau élevé)

  Si la connexion RBSU est requise, les menus de configuration actifs sont contrôlés par les droits d'accès de l'utilisateur authentifié.

- RBSU Disabled (RBSU désactivé) (niveau maximal)

  Lorsque iLO 2 RBSU est désactivé, l'accès utilisateur n'est pas autorisé. Cela empêche toute modification à l'aide de l'interface RBSU.

Administration du commutateur de neutralisation de la sécurité iLO 2

Le commutateur de neutralisation de la sécurité iLO 2 permet à l'administrateur d'accéder intégralement au processeur iLO 2. Cela peut être nécessaire dans les cas suivants :

- la carte iLO 2 doit être réactivée après avoir été désactivée ;
- tous les comptes utilisateur dotés du privilège Administer User Accounts (Administrer comptes utilisateur) ont été verrouillés ;
- une configuration erronée empêche la carte iLO 2 d'apparaître sur le réseau et l'utilitaire RBSU a été désactivé ;
- le bloc d'initialisation doit être flashé.

L'utilisation du commutateur de neutralisation de la sécurité a les conséquences suivantes :

- tous les contrôles d'autorisation de sécurité sont désactivés lorsque le commutateur est activé ;
- l'utilitaire iLO 2 RBSU s'exécute en cas de réinitialisation du serveur hôte ;
- la carte iLO 2 n'est pas désactivée et peut apparaître sur le réseau comme étant configurée ;
- si la carte iLO 2 est désactivée pendant que le commutateur de neutralisation est actif, elle n'est plus en mesure de déconnecter l'utilisateur ni de terminer le processus et cela jusqu'au prochain cycle de mise hors/sous tension du serveur ;
- le bloc d'initialisation est exposé à la programmation.

Un message d'avertissement s'affiche sur les pages du navigateur iLO 2, indiquant que le commutateur de neutralisation de la sécurité iLO 2 est en cours d'utilisation. Une entrée est ajoutée au journal iLO 2 pour enregistrer l'utilisation de ce commutateur. Une alerte SNMP peut également être envoyée après activation ou désactivation de celui-ci.

L'activation du commutateur de neutralisation de la sécurité iLO 2 permet également de flasher le bloc d'initialisation iLO 2. HP ne prévoit pas que vous aurez besoin de mettre à jour le bloc d'initialisation iLO 2. Si une mise à jour du bloc d'initialisation de iLO 2 se révélait être nécessaire, il faudrait se déplacer jusqu'au serveur physique afin de reprogrammer le bloc d'initialisation et de réinitialiser iLO 2. Le bloc d'initialisation sera exposé tant que iLO 2 n'aura pas été réinitialisée. Pour une sécurité optimale, HP vous recommande de déconnecter la carte iLO 2 du réseau tant que la réinitialisation n'est pas terminée. Le commutateur de neutralisation de la sécurité iLO 2 se trouve à l'intérieur du serveur. Vous ne pouvez dès lors pas y accéder sans ouvrir le boîtier du serveur.

Pour paramétrer le commutateur de neutralisation de la sécurité iLO 2 :

1. Mettez le serveur hors tension.
2. Paramétrez le commutateur.
3. Mettez le serveur sous tension.

Inversez la procédure pour désactiver le commutateur de neutralisation de la sécurité iLO 2.

Selon le serveur utilisé, le commutateur de neutralisation de la sécurité iLO 2 peut être un simple cavalier ou une position spécifique sur un panneau de commutateurs à positions multiples. Pour le localiser et y accéder, reportez-vous à la documentation de votre serveur. Vous pouvez également utiliser les diagrammes figurant sur le panneau d'accès du serveur.

Prise en charge du module TPM (Trusted Platform Module)

Le module TPM correspond à une fonction matérielle destinée à sécuriser le système. Cette puce informatique permet de stocker en toute sécurité les informations d'authentification de la plate-forme, à savoir les mots de passe, les certificats ou les clés de codage. Vous pouvez aussi utiliser une puce TPM afin de stocker les mesures relatives à la plate-forme, lesquelles sont destinées à garantir la fiabilité de la plate-forme. iLO 2 permet la prise en charge du module mezzanine TPM sur les serveurs ProLiant 100 et ProLiant 300/500.

Sur un système compatible, iLO 2 décode l'enregistrement TPM et envoie l'état de la configuration vers iLO, l'interface CLP ou XML. L'état de la configuration TPM apparaît dans la page System Status (État du système). Lorsque le module TPM n'est pas pris en charge sur le système hôte ou la ROM système, son état n'est pas indiqué dans la page Status Summary (Récapitulatif de l'état). Cette page propose les informations d'état de module TPM suivantes :

- Not Present (Absent) : aucun module TPM n'est installé.
- Present (Présent) : lorsque :
  - Un module TPM est installé, mais est désactivé.
  - Un module TPM est installé et activé.
  - Un module TPM est installé, activé et une mesure de ROM d'extension est activée. Lorsque cette mesure est activée, si vous cliquez sur **Send firmware image** (Envoyer image du microprogramme), un message d'avertissement s'affiche dans la page Update iLO2 Firmware (Mettre à jour le microprogramme iLO 2).

Comptes et accès utilisateur

La carte iLO 2 prend en charge la configuration de 12 comptes utilisateur locaux maximum. Chacun de ces comptes peut être géré par l'intermédiaire des éléments suivants :

- Privilèges (Privilèges à la page 44)
- Sécurité de la connexion (Sécurité de la connexion à la page 44)

iLO 2 peut être configuré afin d'utiliser un annuaire pour authentifier et autoriser ses utilisateurs. Cette configuration autorise l'intégration d'un nombre quasi illimité d'utilisateurs et s'adapte aisément au nombre de périphériques Lights-Out d'une entreprise. En outre, l'annuaire fournit un point central d'administration aux utilisateurs et périphériques Lights-Out et peut faire appliquer une stratégie de mot de passe plus stricte. iLO 2 permet d'intégrer des utilisateurs locaux, d'annuaire ou les deux.

Deux options de configuration sont disponibles : à l'aide d'un annuaire étendu au moyen du schéma HP (Configuration de l'intégration d'annuaire dans le cadre du schéma HP à la page 157) ou à l'aide du

schéma d'annuaire par défaut (Configuration pour l'intégration d'annuaire sans schéma à la page 153).

Privilèges

La carte iLO 2 permet à l'administrateur de contrôler l'accès des comptes utilisateur aux fonctions iLO 2 par l'intermédiaire de privilèges. Lorsqu'un utilisateur essaie d'utiliser une fonction, le système iLO 2 vérifie s'il dispose du privilège requis avant de l'autoriser à se servir de la fonction.

Toutes les fonctions disponibles via la carte iLO 2 sont contrôlables via des privilèges, y compris Administer User Accounts (Administrer comptes utilisateur), Remote Console Access (Accès console distante), Virtual Power and Reset (Alimentation et réinitialisation virtuelles), Virtual Media (Support virtuel) et Configure iLO 2 Settings (Configurer paramètres iLO 2). Vous pouvez configurer les privilèges pour chaque utilisateur sur la page User Administration (Administration des utilisateurs) de l'onglet Administration.

Sécurité de la connexion

La carte iLO 2 propose plusieurs fonctions pour assurer la sécurité de la connexion. Après l'échec d'une tentative initiale d'ouverture de session, la carte iLO 2 impose un temps d'attente de cinq secondes. Après l'échec de la deuxième tentative, la carte iLO 2 impose un temps d'attente de dix secondes. Après l'échec de la troisième tentative, la carte iLO 2 impose un délai de 60 secondes. En cas d'échec des tentatives d'ouverture de session suivantes, les délais d'attente suivent le même cycle. Une page d'information s'affiche pendant chaque délai d'attente. Le processus se poursuit jusqu'à l'ouverture d'une session valide. Cette fonction contribue à une défense contre des attaques éventuelles à l'encontre du port de connexion du navigateur.

La carte iLO 2 enregistre par ailleurs une entrée de journal détaillée pour les tentatives de connexion non abouties imposant un délai de 60 secondes.

Administration de clé SSH

À l'aide de l'onglet SSH Key (Clé SSH), iLO 2 permet d'utiliser jusqu'à quatre clés SSH à la fois. Cet onglet affiche également le propriétaire (si les clés sont autorisées) de chaque clé autorisée SSH. Plusieurs clés peuvent appartenir à un seul utilisateur.

Pour ajouter une clé autorisée à iLO 2, le chemin de la clé publique doit être soumis à iLO 2. Le fichier de clé doit contenir le nom de l'utilisateur à la fin de la clé. Chaque clé est associée à un compte utilisateur local. Si le compte local n'existe pas ou s'il a été supprimé, la clé n'est pas valide (la clé n'est pas répertoriée si le compte local n'existe pas).

Vous pouvez également autoriser les clés SSH pour un serveur HP SIM en lançant l'outil mxagentconfig à partir du serveur HP SIM et en indiquant l'adresse et les données utilisateur pour iLO 2. Pour plus d'informations, reportez-vous à la documentation relative aux produits HP SIM.

Pour autoriser une nouvelle clé :

1. Dans l'interface iLO 2, cliquez sur **Administration>Security>SSH Key** (Administration>Sécurité>Clé SSH).
2. Cliquez sur **Browse** (Parcourir) et recherchez le fichier de clé.
3. Cliquez sur **Authorize Key** (Autoriser la clé).

Vous pouvez afficher ou supprimer toute clé précédemment autorisée en sélectionnant une clé et en cliquant sur **View Selected Key** (Afficher clé sélectionnée) ou **Delete Selected Key** (Supprimer clé sélectionnée). Ces boutons s'affichent uniquement lorsque les clés SSH sont installées.

Administration des certificats SSL

iLO 2 permet de créer une demande de certificat, d'importer un certificat et d'afficher les informations d'administration du certificat associées à un certificat stocké. Ces informations sont codées dans le certificat par l'autorité de certification et sont extraites par la carte iLO 2.

Par défaut, iLO 2 crée un certificat « à signature automatique » utilisable dans les connexions SSL. Ce certificat permet à la carte iLO 2 de fonctionner sans autre étape de configuration. Les fonctions de sécurité iLO 2 peuvent être étendues par l'importation d'un certificat validé. Pour plus d'informations sur les certificats et les services de certificat, reportez-vous aux sections « Introduction aux services de certificat » (Introduction aux services de certificat à la page 153) et « Installation des services de certificat » (Installation des services de certificat à la page 153).

Pour accéder aux informations de certificat, cliquez sur **Administration>Security>SSL Certificate** (Administration>Sécurité>Certificat SSL). L'onglet SSL Certificate (Certificat SSL) affiche les informations suivantes :

- Le champ Issued To (Envoyé à) contient l'entité vers laquelle le certificat a été envoyé.
- Le champ Issued By (Emis par) répertorie l'autorité de certification émettrice du certificat.
- Le champ Valid From (Valide depuis) indique la première date à laquelle le certificat est valide.
- Le champ Valid Until (Valide jusqu'au) affiche la date d'expiration du certificat.
- Le champ Serial Number (Numéro de série) contient le numéro de série attribué au certificat par l'autorité de certification.

Les options suivantes sont disponibles dans l'onglet SSL Certificate (Certificat SSL) :

- Create Certificate Request (Créer demande de certificat) : ce bouton permet de créer une demande de certificat. Lorsque vous cliquez sur ce bouton, une demande de certificat est créée (au format PKCS #10) et peut être envoyée à l'autorité de certification. Cette demande de certificat est codée en Base64. Une autorité de certification traite cette demande et envoie une réponse (certificat X. 509) qui peut être importée dans iLO 2.

  La demande de certificat contient le code et le certificat public/privé validant les communications entre le navigateur client et iLO 2. La demande générée est conservée jusqu'à la génération d'une nouvelle demande, la réinitialisation de iLO 2 ou l'importation d'un certificat par le processus de génération. Vous pouvez générer la demande de certificat et la copier dans le presse-papiers du client, quitter le site Web iLO 2 pour rechercher le certificat, puis revenir pour importer le certificat.

  Lors de la soumission d'une demande à une autorité de certification, assurez-vous :

  a. d'utiliser le nom iLO 2 répertorié dans l'écran System Status (État du système) en tant qu'URL du serveur ;

  b. de demander que le certificat soit généré au format RAW ;

  c. d'inclure les lignes `Begin` (Début) et `End` (Fin) du certificat.

  Chaque fois que vous cliquez sur le bouton **Create Certificate Request** (Créer demande de certificat), une nouvelle demande de certificat est générée, même si le nom de la carte iLO 2 est le même.

- Import Certificate (Importer certificat) : utilisez ce bouton pour revenir à la page Certificate Administration (Administration de certificats) contenant un certificat à importer. Cliquez sur **Import Certificate** (Importer certificat) pour accéder directement à l'écran Certificate Import (Importer certificat) sans générer de nouvelle demande de certificat. Un certificat ne fonctionne qu'avec les clés générées pour la demande de certificat originale à partir de laquelle le certificat a été généré. Lorsque iLO 2 a été réinitialisé ou qu'une autre demande de certificat a été générée depuis la

soumission de la demande originale à une autorité de certification, la nouvelle demande de certificat doit être générée et soumise à l'autorité de certification.

Vous pouvez créer une demande de certificat ou importer un certificat existant en utilisant les commandes XML RIBCL. Ces commandes permettent de générer le script et de déployer automatiquement des certificats des serveurs iLO 2 au lieu de les déployer manuellement via l'interface du navigateur. Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Authentification à deux facteurs

Pour accéder à iLO 2, l'utilisateur doit s'authentifier. Cette version du microprogramme propose une structure d'authentification améliorée pour la carte iLO 2, grâce à deux facteurs d'authentification : un mot de passe ou code d'identification personnel (PIN) et une clé privée pour un certificat numérique. Une authentification à deux facteurs implique que vous validiez votre identité en donnant les deux facteurs. Vous pouvez stocker vos certificats numériques et vos clés privées où vous le souhaitez, dans une carte à puce, une clé USB ou un disque dur par exemple.

L'onglet Two-Factor Authentication (Authentification à deux facteurs) permet de configurer les paramètres de sécurité et de consulter, importer ou supprimer une autorité de certification agréée. Le paramètre Two-Factor Authentication Enforcement (Renforcement de l'authentification à deux facteurs) détermine si l'authentification à deux facteurs doit être utilisée pour l'authentification utilisateur pendant la procédure d'identification. Pour demander une authentification à deux facteurs, cliquez sur **Enabled** (Activé). Pour désactiver l'authentification à deux facteurs et permettre l'identification avec le nom d'utilisateur et le mot de passe uniquement, cliquez sur **Disabled** (Désactivé). Vous ne pouvez pas définir ce paramètre sur Enabled (Activé) lorsqu'aucun certificat provenant d'une autorité de certification agréée n'a été configuré. Pour des raisons de sécurité, les modifications suivantes sont apportées à la configuration lorsque l'authentification à deux facteurs est activée :

- Telnet Access (Accès Telnet) : Disabled (Désactivé)
- Secure Shell (SSH) Access (Accès SSH) : Disabled (Désactivé)
- Serial Command Line Interface Status (État de l'interface de ligne de commande série) : Disabled (Désactivé)

Si l'accès requiert Telnet, SSH ou une interface de ligne de commande série, réactivez ces paramètres une fois que l'authentification à deux facteurs a été activée. Toutefois, ces méthodes d'accès n'offrant pas la possibilité d'une authentification à deux facteurs, seul un facteur est requis lors de l'accès à iLO 2 avec Telnet, SSH ou une interface de ligne de commande série.

Lorsque l'authentification à deux facteurs est activée, l'accès via l'utilitaire CPQLOCFG est désactivé car ce dernier ne répond pas à toutes les conditions requises par l'authentification. En revanche, l'utilitaire HPONCFG est opérationnel car son exécution requiert des privilèges d'administrateur sur le système hôte.

Un certificat provenant d'une autorité de certification agréée est nécessaire au fonctionnement de l'authentification à deux facteurs. Vous ne pouvez pas définir le paramètre Two-Factor Authentication Enforcement (Renforcement de l'authentification à deux facteurs) sur Enabled (Activé) si aucun certificat provenant d'une autorité de certification agréée n'a été configuré. De plus, si des comptes utilisateur locaux sont utilisés, vous devez associer un certificat client au compte utilisateur local. Lorsque iLO 2 utilise l'authentification d'annuaires, l'association des certificats client aux comptes d'utilisateurs locaux est facultative.

Pour modifier les paramètres de sécurité de l'authentification à deux facteurs pour iLO 2, procédez comme suit :

1. Connectez-vous à la carte iLO 2 en utilisant un compte doté du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2).
2. Cliquez sur **Administration>Security>Two-Factor Authentication** (Administration>Sécurité>Authentification à deux facteurs).
3. Modifiez les paramètres en renseignant les champs adéquats.
4. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Le paramètre Certificate Revocation Checking (Contrôle de la révocation de certificat) permet de contrôler si iLO 2 utilise l'attribut des points de distribution de la liste des révocations de certificat pour télécharger la dernière version de cette liste et vérifier les révocations du certificat client. Si le certificat client se trouve dans la liste des révocations de certificat ou si vous ne pouvez pas télécharger cette liste, l'accès est refusé. Le point de distribution de la liste des révocations de certificat doit être disponible et accessible pour iLO 2 lorsque vous définissez le paramètre Certificate Revocation Checking (Contrôle de la révocation de certificat) sur **Yes** (Oui).

Le paramètre Certificate Owner Field (Champ du propriétaire du certificat) indique l'attribut de certificat client à utiliser pour l'authentification par rapport à l'annuaire. Utilisez uniquement ce paramètre si l'authentification d'annuaire est activée. La configuration de ce paramètre dépend de la version de la prise en charge d'annuaires utilisée, de la configuration des annuaires et de la politique de délivrance de certificats de votre entreprise. Lorsque SAN (Réseau SAN) est défini, iLO 2 extrait la valeur de User Principle Name (Nom principal de l'utilisateur) de l'attribut Subject Alternative Name (Nom alternatif de l'objet) et utilise le nom principal de l'utilisateur lors de l'authentification d'annuaires (par exemple, nomd'utilisateur@domaine.extension). Par exemple, si le nom d'objet est `/DC=com/DC=domain/OU=organization/CN=user`, iLO 2 déduit `CN=user, OU=organization, DC=domain, DC=com`.

Configuration de l'authentification à deux facteurs pour la première fois

Lorsque vous configurez l'authentification à deux facteurs pour la première fois, vous pouvez utiliser des comptes utilisateur locaux ou des comptes utilisateur d'annuaires. Pour plus d'informations sur les paramètres de l'authentification à deux facteurs, reportez-vous à la section « Authentification à deux facteurs » (Authentification à deux facteurs à la page 46).

Configuration des comptes utilisateur locaux

1. Obtenez le certificat public auprès de l'autorité de certification qui délivre les certificats utilisateur ou les cartes à puce dans votre entreprise.
2. Exportez le certificat au format codé en Base64 dans un fichier sur votre bureau, par exemple CAcert.txt.
3. Procurez-vous le certificat public de l'utilisateur qui doit accéder à iLO 2.
4. Exportez le certificat au format codé en base64 dans un fichier sur votre bureau, par exemple Usercert.txt.
5. Ouvrez le fichier CAcert.txt dans le Bloc-notes, sélectionnez tout le texte et copiez-le en appuyant sur les touches **Ctrl+C**.
6. Connectez-vous à la carte iLO 2 et naviguez jusqu'à la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs).
7. Cliquez sur **Import Trusted CA Certificate** (Importer le certificat validé par l'autorité de certification). La page Import Root CA Certificate s'affiche.

8. Cliquez dans la zone de texte blanche afin d'y placer votre curseur, puis collez le contenu du Presse-papiers en appuyant sur les touches **Ctrl+V**.
9. Cliquez sur **Import Root CA Certificate** (Importer le certificat racine de l'autorité de certification). La page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs) s'affiche à nouveau, avec les informations indiquées sous Trusted CA Certificate Information (Informations sur le certificat validé par l'autorité de certification).
10. À partir de votre bureau, ouvrez le fichier du certificat utilisateur dans le Bloc-notes, sélectionnez tout le texte et copiez-le dans le Presse-papiers en appuyant sur les touches **Ctrl+C**.
11. Naviguez jusqu'à la page User Administration (Administration des utilisateurs) dans iLO 2 et sélectionnez l'utilisateur pour lequel vous avez obtenu un certificat public ou créez un nouvel utilisateur.
12. Cliquez sur **View/Modify** (Afficher/Modifier).
13. Cliquez sur **Add a certificate** (Ajouter un certificat).
14. Cliquez dans la zone de texte blanche afin d'y placer votre curseur, puis collez le contenu du Presse-papiers en appuyant sur les touches **Ctrl+V**.
15. Cliquez sur **Add user Certificate** (Ajouter un certificat utilisateur). La page Modify User (Modifier utilisateur) s'affiche à nouveau, avec un nombre à 40 chiffres dans le champ Thumbprint (Empreinte). Vous pouvez comparer le nombre à l'empreinte affichée pour le certificat grâce à Microsoft® Certificate Viewer.
16. Naviguez jusqu'à la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs).
17. Sélectionnez **Enabled** (Activé) pour l'option Two-Factor Authentication (Authentification à deux facteurs).
18. Sélectionnez **Disabled** (Désactivé) pour l'option Certificate Revocation Checking (Contrôle de la révocation de certificat). Cette option est la valeur par défaut.
19. Cliquez sur **Apply** (Appliquer). iLO 2 est réinitialisé. Lorsque iLO 2 tente d'atteindre à nouveau la page d'identification, le navigateur affiche la page Client Authentication (Authentification client), avec une liste des certificats disponibles pour le système.

    Si le certificat utilisateur n'est pas enregistré sur la machine client, vous ne pouvez pas le voir dans la liste. Le certificat utilisateur doit être enregistré sur le système client pour que vous puissiez le voir. Lorsqu'il n'y a aucun certificat client sur le système client, il est possible que vous n'obteniez pas la page Client Authentication (Authentification client), mais plutôt une page d'erreur indiquant « Page cannot be displayed » (Impossible d'afficher la page). Pour pallier à cela, vous devez enregistrer le certificat client sur la machine client. Pour plus d'informations sur l'exportation et l'enregistrement de certificats client, reportez-vous à la documentation de votre carte à puce ou contactez votre autorité de certification.
20. Sélectionnez le certificat ajouté à l'utilisateur dans iLO 2. Cliquez sur **OK**.
21. Si vous y êtes invité, insérez la carte à puce ou saisissez votre code d'identification personnel ou mot de passe.

Une fois que vous avez terminé le processus d'authentification, vous avez accès à la carte iLO 2.

Configuration des comptes utilisateur d'annuaire

1. Obtenez le certificat public auprès de l'autorité de certification qui délivre les certificats utilisateur ou les cartes à puce dans votre entreprise.
2. Exportez le certificat au format codé en Base64 dans un fichier sur votre bureau, par exemple CAcert.txt.
3. Ouvrez le fichier dans le Bloc-notes, sélectionnez tout le texte et copiez-le dans le Presse-papiers en appuyant sur les touches **Ctrl+C**.
4. Connectez-vous à la carte iLO 2 et naviguez jusqu'à la page **Two-Factor Authentication Settings** (Paramètres d'authentification à deux facteurs).
5. Cliquez sur **Import Trusted CA Certificate** (Importer le certificat validé par l'autorité de certification). Une autre page s'affiche.
6. Cliquez dans la zone de texte blanche afin d'y placer votre curseur, puis collez le contenu du Presse-papiers en appuyant sur les touches **Ctrl+V**.
7. Cliquez sur **Import Root CA Certificate** (Importer le certificat racine de l'autorité de certification). La page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs) s'affiche à nouveau, avec les informations indiquées sous Trusted CA Certificate Information (Informations sur le certificat validé par l'autorité de certification).
8. Attribuez la valeur **Yes** (Oui) au paramètre Enforce Two-Factor Authentication (Appliquer l'authentification à deux facteurs).
9. Définissez Certificate Revocation Checking (Contrôle de la révocation de certificat) sur **No (default)** (Non [par défaut]).
10. Attribuez au paramètre Certificate Owner Field (Champ du propriétaire du certificat) la valeur **SAN** (Réseau SAN). Pour plus d'informations, reportez-vous à la section « Authentification à deux facteurs » (Authentification à deux facteurs à la page 46).
11. Cliquez sur **Apply** (Appliquer). iLO 2 est réinitialisé. Lorsque iLO 2 tente d'atteindre à nouveau la page d'identification, le navigateur affiche la page Client Authentication (Authentification client), avec une liste des certificats disponibles pour le système.
12. Sélectionnez le certificat ajouté à l'utilisateur dans iLO 2. Cliquez sur **OK**.
13. Si vous y êtes invité, insérez la carte à puce ou saisissez votre code d'identification personnel ou mot de passe. La page d'identification doit s'afficher avec l'adresse e-mail de l'utilisateur dans le champ Directory User (Utilisateur de l'annuaire). Vous ne pouvez pas modifier ce paramètre.
14. Saisissez le mot de passe de l'utilisateur de l'annuaire. Cliquez sur **Login** (Connexion).

Une fois le processus d'authentification terminé, vous pouvez accéder à iLO 2. Pour plus d'informations sur la configuration des utilisateurs des annuaires et des privilèges, reportez-vous à la section « Paramètres d'annuaire » (Directory Settings (Paramètres d'annuaire) à la page 52).

Configuration d'un utilisateur pour une authentification à deux facteurs

Pour authentifier un utilisateur avec un compte iLO 2 local, un certificat doit être associé au nom de l'utilisateur local. Dans la page Administration>Modify User (Administration>Modifier utilisateur), lorsqu'un certificat a été associé à l'utilisateur, une empreinte (un hachage SHA1 du certificat) s'affiche, ainsi qu'un bouton permettant de supprimer le certificat. Si aucun certificat n'a été associé à l'utilisateur, le message `Thumbprint: A certificate has NOT been mapped to this user` (Empreinte : aucun certificat associé à cet utilisateur) s'affiche, avec un bouton qui permet de démarrer le processus d'importation du certificat.

Pour définir un utilisateur pour l'authentification à deux facteurs et ajouter un certificat utilisateur :

1. Connectez-vous à la carte iLO 2 en utilisant un compte doté du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2).
2. Cliquez sur **Administration>User Administration** (Administration>Administration des utilisateurs). Sélectionnez un utilisateur.
3. Cliquez sur **View/Modify** (Afficher/Modifier).
4. Dans la section User Certificate Information (Informations sur le certificat utilisateur), cliquez sur **Add a certificate** (Ajouter un certificat).
5. Dans la page Map User Certificate (Associer un certificat utilisateur), collez le certificat utilisateur dans la zone de texte, puis cliquez sur **Import Certificate** (Importer certificat). Pour plus d'informations sur la création, la copie et le collage des informations des certificats, reportez-vous à la section « Configuration de l'authentification à deux facteurs pour la première fois » (Configuration de l'authentification à deux facteurs pour la première fois à la page 47).

Connexion avec l'authentification à deux facteurs

Lorsque vous vous connectez à la carte iLO 2 et que l'authentification à deux facteurs est requise, la page Client Authentication (Authentification client) vous invite à sélectionner le certificat à utiliser. Elle répertorie ensuite tous les certificats disponibles pour authentifier un client. Sélectionnez votre certificat. Le certificat peut être un certificat associé à un utilisateur local dans iLO 2 ou un certificat spécifique à l'utilisateur et émis pour l'authentification dans le domaine.



Une fois que vous avez sélectionné un certificat, si ce dernier est protégé par mot de passe ou stocké sur une carte à puce, une deuxième page s'affiche et vous invite à saisir le code d'identification personnel ou mot de passe associé au certificat choisi.



iLO 2 examine le certificat pour garantir qu'il a été émis par une autorité de certification agréée en comparant la signature de cette autorité à celle configurée dans iLO 2. iLO 2 détermine si le certificat a été supprimé ou non, et s'il est associé à un utilisateur de la base de données locale des utilisateurs de iLO 2. Lorsque tous ces tests sont concluants, l'interface utilisateur iLO 2 classique s'affiche.

Si l'authentification de vos informations d'identification échoue, la page d'échec de connexion s'affiche. Dans ce cas, vous êtes invité à fermer le navigateur, ouvrir une nouvelle page du navigateur et réessayer. Lorsque l'authentification d'annuaires est activée et que l'authentification de l'utilisateur local échoue, iLO 2 affiche une page de connexion dans laquelle la valeur du champ du nom d'utilisateur dans l'annuaire correspond à la valeur du paramètre User Principal Name (Nom principal de l'utilisateur) du certificat ou à celle du paramètre Distinguished name (Nom distinctif) (dérivé de l'objet du certificat). iLO 2 demande le mot de passe pour ce compte. Une fois que vous avez fourni le mot de passe, vous êtes authentifié.

Utilisation de l'authentification à deux facteurs avec l'authentification d'annuaire

Dans certains cas, la configuration de l'authentification à deux facteurs avec l'authentification d'annuaires est compliquée. iLO 2 peut utiliser le schéma HP Extended ou le schéma Default Directory pour l'intégration aux services d'annuaires. Pour assurer la sécurité lorsque l'authentification à deux facteurs est renforcée, iLO 2 utilise un attribut du certificat client en tant que nom de connexion de l'utilisateur à l'annuaire. Le paramètre de configuration qui détermine l'attribut de certificat client à utiliser par iLO 2 est Certificate Owner (Propriétaire du certificat) sur la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs). Lorsque la valeur attribuée à ce paramètre est SAN (Réseau SAN), iLO 2 obtient le nom de connexion de l'utilisateur à l'annuaire à partir de l'attribut UPN du réseau SAN. Lorsque le paramètre Certificate Owner (Propriétaire du certificat) est défini sur la valeur Subject (Objet), iLO 2 obtient le nom distinctif de l'utilisateur dans l'annuaire à partir de l'objet du certificat.

La valeur attribuée à ce champ dépend de la méthode utilisée pour l'intégration de l'annuaire, de la structure de l'annuaire et des informations contenues dans les certificats utilisateurs émis. Les exemples suivants présupposent que vous disposez des autorisations appropriées.

Authentification à l'aide du schéma Default Directory, partie 1 : le nom distinctif d'un utilisateur dans l'annuaire est CN=John Doe, OU=IT, DC=MyCompany, DC=com et les attributs du certificat de John Doe sont les suivants :

- Subject: DC=com/DC=MyCompany/OU=IT/CN=John Doe
- SAN/UPN: john.doe@MyCompany.com

L'authentification auprès d'iLO 2 avec le nom d'utilisateur john.doe@MyCompany.com et le mot de passe fonctionne si l'authentification à deux facteurs n'a **pas** été appliquée. Lorsque l'authentification à deux facteurs est appliquée, si la valeur SAN (Réseau SAN) est sélectionnée dans la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs), la valeur john.doe@MyCompany.com apparaît automatiquement dans le champ Directory User (Utilisateur d'annuaire) de la page de connexion. Le mot de passe peut être saisi, mais l'utilisateur ne sera **pas** authentifié. En effet, john.doe@MyCompany.com, qui a été obtenu à partir du certificat, n'est pas le nom distinctif de l'utilisateur dans l'annuaire. Dans ce cas, vous devez sélectionner la valeur **Subject**

(Objet) dans la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs). Le champ Directory User (Utilisateur d'annuaire) est alors automatiquement renseigné avec la valeur CN=John Doe,OU=IT,DC=MyCompany,DC=com, ce qui correspond au nom distinctif réel de l'utilisateur. Si le mot de passe saisi est correct, l'utilisateur est authentifié.

Authentification à l'aide du schéma Default Directory, partie 2 : le nom distinctif d'un utilisateur dans l'annuaire est CN=john.doe@MyCompany.com, OU=IT, DC=MyCompany, DC=com et les attributs du certificat de John Doe sont les suivants :

- Subject: DC=com/DC=MyCompany/OU=Employees/CN=John Doe/ E=john.doe@MyCompany.com
- SAN/UPN: john.doe@MyCompany.com
- Le contexte de recherche sur la page Directory Settings (Paramètres d'annuaire) est défini sur : OU=IT,DC=MyCompany,DC=com

Dans cet exemple, si la valeur SAN (Réseau SAN) est sélectionnée sur la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs), le champ Directory User (Utilisateur d'annuaire) de la page d'ouverture de session est renseigné avec la valeur john.doe@MyCompany.com. Une fois que le mot de passe correct est saisi, l'utilisateur est authentifié. Il est authentifié même si john.doe@MyCompany.com n'est pas son nom distinctif. En effet, iLO 2 tente de l'authentifier à l'aide des champs du contexte de recherche (CN=john.doe@MyCompany.com, OU=IT, DC=MyCompany, DC=com) configurés dans la page Directory Settings (Paramètres d'annuaire). Comme il s'agit du nom distinctif correct de l'utilisateur, iLO 2 le retrouve dans l'annuaire.

REMARQUE : si vous sélectionnez Subject (Objet) dans la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs), l'authentification échoue car l'objet du certificat ne constitue pas le nom distinctif de l'utilisateur dans l'annuaire.

Lorsque vous utilisez la méthode de schéma HP Extended pour l'authentification, HP recommande de sélectionner l'option SAN (Réseau SAN) dans la page Two-factor Authentication Settings (Paramètres d'authentification à deux facteurs).

Directory Settings (Paramètres d'annuaire)

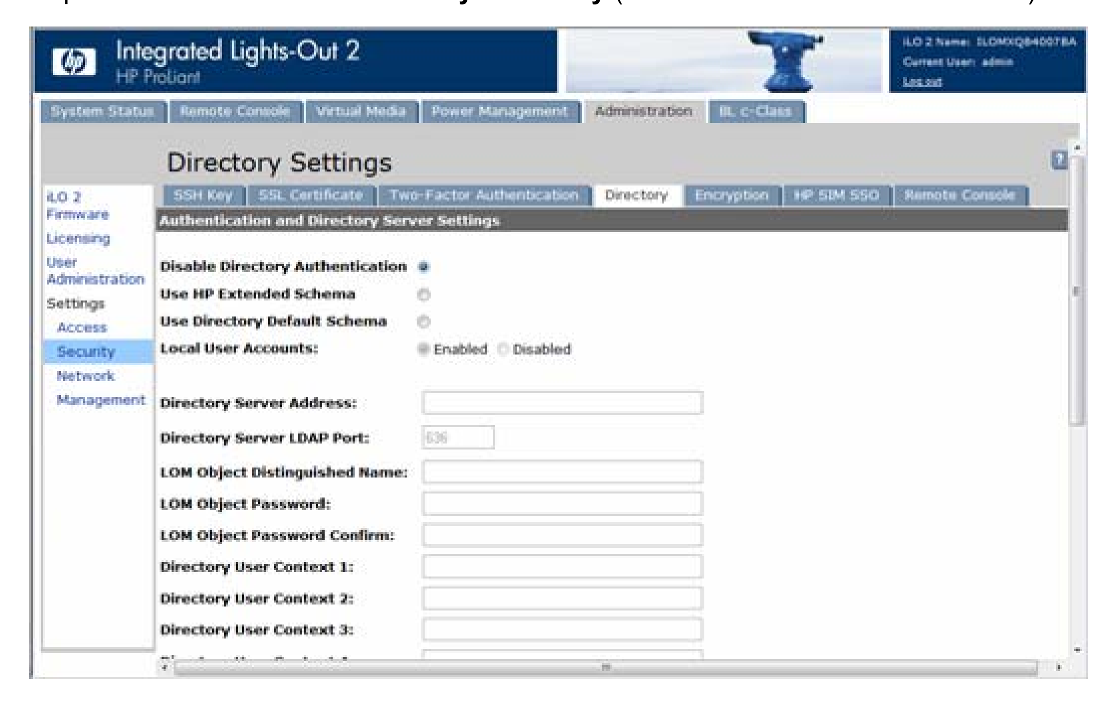
iLO 2 se connecte aux services d'annuaire Microsoft® Active Directory, Novell e-Directory et autres services d'annuaire compatibles LDAP 3.0 pour l'authentification et l'autorisation d'utilisateurs. Vous pouvez configurer iLO 2 pour authentifier et autoriser des utilisateurs en utilisant l'intégration d'annuaires de schéma HP ou l'intégration d'annuaires sans schéma. ILO 2 se connecte uniquement aux services d'annuaire en employant des connexions sécurisées SSL vers le port LDAP du serveur d'annuaires. Le port LDAP sécurisé par défaut est 636. La prise en charge des services d'annuaire est une fonction sous licence disponible avec l'achat de licences facultatives. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21). Pour plus d'informations sur les annuaires, reportez-vous à la section « Services d'annuaire » (Services d'annuaire à la page 149).

Les comptes utilisateur stockés localement, trouvés sur la page User Administration (Administration des utilisateurs), peuvent êtres actifs lorsque la prise en charge d'annuaires iLO 2 est activée. Cette prise en charge active les accès utilisateur locaux et basés sur les annuaires. Généralement, un administrateur peut supprimer des comptes utilisateur locaux (excepté, peut-être un compte d'accès d'urgence) une fois que iLO 2 est correctement configuré pour accéder au service d'annuaire. Vous pouvez également désactiver l'accès à ces comptes si la prise en charge d'annuaires est activée.

Configuration des paramètres d'annuaire

iLO 2 permet aux administrateurs de centraliser l'administration des comptes utilisateur à l'aide des services d'annuaire. Vous devez disposer du privilège Configure iLO 2 Settings (Configurer paramètres

iLO 2) pour configurer et tester les services d'annuaire iLO 2. Pour accéder aux paramètres d'annuaire, cliquez sur **Administration>Security>Directory** (Administration>Sécurité>Annuaire).



Les paramètres iLO 2 permettent de contrôler le comportement de l'annuaire iLO 2 auquel vous êtes connecté. Ces paramètres comprennent :

- Disable Directory Authentication (Désactiver authentification de l'annuaire) : permet d'activer ou de désactiver la prise en charge de l'annuaire sur cet annuaire iLO 2.
  - Si l'authentification d'annuaire est activée et correctement configurée, les utilisateurs peuvent se connecter à l'aide des données d'authentification de l'annuaire.
  - Dans le cas contraire, les données d'authentification de l'utilisateur ne sont pas validées lors de l'utilisation de l'annuaire.
- Use HP Extended Schema (Utiliser schéma HP Extended) : permet de sélectionner une authentification d'annuaire et une autorisation à l'aide des objets d'annuaire créés avec le schéma HP. Sélectionnez cette option si l'annuaire a été étendu par le schéma HP et si vous en avez besoin.
- Use Directory Default Schema (Utiliser le schéma Directory Default) : permet de sélectionner une authentification d'annuaire et une autorisation à l'aide des comptes utilisateur de l'annuaire. Sélectionnez cette option si l'annuaire n'est pas étendu par le schéma HP. Les comptes utilisateur et le nombre des membres du groupe servent à authentifier et autoriser les utilisateurs. Après avoir entré les informations du réseau d'annuaires, cliquez sur **Administer Groups** (Administrer les groupes). Entrez un ou plusieurs noms distinctifs d'annuaire valides ainsi que les privilèges d'accès à iLO 2.
- Enable Local User Accounts (Activer les comptes utilisateur locaux) : permet de limiter l'accès aux utilisateurs locaux.
  - Si ce paramètre est activé, un utilisateur peut se connecter à l'aide de ses données d'authentification stockées localement.
  - Dans le cas contraire, l'accès de l'utilisateur se limite uniquement aux données valides d'authentification de l'annuaire.

L'accès utilisant les comptes utilisateur locaux est activé si Directory Support (Prise en charge des annuaires) est désactivé et/ou si la licence de iLO 2 ou iLO 2 Advanced est supprimée. Vous ne pouvez pas désactiver l'accès de l'utilisateur local si vous êtes connecté via un compte utilisateur local.

Les paramètres du serveur d'annuaires iLO 2 permettent d'identifier son adresse et son port. Ces paramètres comprennent :

- Directory Server Address (Adresse du serveur d'annuaires) : permet de définir le nom DNS du réseau ou l'adresse IP du serveur d'annuaires. Vous pouvez indiquer plusieurs serveurs en les séparant par une virgule (,) ou un espace ( ). Si Use Directory Default Schema (Utiliser le schéma Directory Default) est sélectionné, entrez un nom DNS dans le champ Directory Server Address (Adresse du serveur d'annuaires) pour permettre une authentification avec l'ID de l'utilisateur. Par exemple :

```
directory.hp.com
192.168.1.250, 192.168.1.251
```

- Directory Server LDAP Port (Port LDAP du serveur d'annuaires) : indique le numéro de port du service LDAP sécurisé sur le serveur. La valeur par défaut de ce port est 636. Cependant, vous pouvez définir une valeur différente si le service d'annuaire est configuré pour utiliser un port différent.
- iLO 2 Directory Properties (Propriétés d'annuaires iLO 2) : indique l'objet LOM dans l'arborescence d'annuaires. Ces informations permettent de définir les droits d'accès de l'utilisateur. iLO 2 peut être configuré avec le mot de passe de l'objet LOM. Cependant, il n'est pas utilisé tant que la prise en charge de la configuration de l'annuaire n'est pas fournie.
- LOM Object Distinguished Name (Nom distinctif de l'objet LOM) : indique où est répertoriée l'instance LOM dans l'arborescence. Par exemple : cn=iLO 2 Mail Server,ou=Management Devices,o=hp.

  Lors d'un accès au serveur d'annuaires, les contextes de recherche utilisateur ne s'appliquent pas au LOM Object Distinguished Name (Nom distinctif de l'objet LOM).
- LOM Object Password (Mot de passe de l'objet LOM) : indique le mot de passe de l'objet utilisé par iLO 2 pour vérifier les mises à jours de l'annuaire (LOM Object Distinguished Name) (Nom distinctif de l'objet LOM).
- Confirm Password (Confirmer mot de passe) : permet de confirmer le mot de passe de l'objet LOM. Si vous le modifiez, entrez le nouveau mot de passe dans ce champ.
- User Login Search Contexts (Contextes de recherche de connexion utilisateur) : vous permettent de définir les sous-contextes d'annuaire communs afin d'éviter aux utilisateurs de rentrer leurs noms distinctifs complets à la connexion.

  Les noms distinctifs sont uniques et permettent d'identifier tous les objets de l'annuaire. Cependant, ils peuvent être longs et les utilisateurs peuvent ne pas les connaître dans leur intégralité ou avoir des comptes dans des contextes d'annuaire différents. iLO 2 essaie de contacter le service d'annuaire en identifiant les noms, puis applique les contextes de recherche jusqu'à trouver une concordance.

  Les contextes utilisateur d'annuaire identifient les contextes du nom d'utilisateur s'appliquant au nom de connexion.

  Exemple 1 :

  Au lieu de se connecter en tant que cn=user, ou=engineering, o=hp, un contexte de recherche `ou=engineering, o=hp` permet de se connecter comme `user`.

Exemple 2 :

Si un système est géré par Information Management, Services, et Training, des contextes de recherche tels que :

```
Directory User Context 1:ou=IM,o=hp
Directory User Context 2:ou=Services,o=hp
Directory User Context 3:ou=Training,o=hp
```

permettent aux utilisateurs de ces organisations de se connecter uniquement à l'aide de ces noms. Si un utilisateur est à la fois présent dans l'unité organisationnelle IM et dans celle Training, la connexion est d'abord essayée avec cn=user,ou=IM,o=hp.

Exemple 3 (Active Directory uniquement) :

Microsoft Active Directory permet d'utiliser un autre format d'authentification utilisateur. Les contextes de recherche dans ce format ne peuvent pas être testés sauf dans le cas d'une tentative de connexion réussie. Un utilisateur peut se connecter en utilisant.

```
user@domain.hp.com
in which case a search context of
@domain.hp.com
allows the user to login as
user
```

Pour tester la communication entre le serveur d'annuaires et la carte iLO 2, cliquez sur **Test Settings** (Tester paramètres). Pour plus d'informations, reportez-vous à la section « Tests d'annuaire » (Tests d'annuaire à la page 55).

Tests d'annuaire

Pour valider les paramètres d'annuaire actuels de la carte iLO 2, cliquez sur **Test Settings** (Tester paramètres) dans la page Directory Settings (Paramètres d'annuaire). La page Directory Tests (Tests d'annuaire) s'affiche.

La page de test affiche les résultats d'une série de tests simples conçus pour valider les paramètres actuels de l'annuaire. Elle inclut en outre un journal de test qui affiche les résultats des tests ainsi que les éventuels problèmes détectés. Vous n'avez pas besoin d'exécuter à nouveau ces tests une fois que vos paramètres d'annuaire sont correctement configurés. L'écran Directory Tests (Tests d'annuaire) n'exige pas que l'utilisateur soit connecté comme un utilisateur d'annuaire.

Pour vérifier vos paramètres d'annuaire :

1. Entrez le nom distinctif et le mot de passe d'un administrateur d'annuaire ; L'idéal serait de prendre les données d'authentification utilisées lors de la création des objets iLO 2 dans l'annuaire. Ces données ne sont pas enregistrées par la carte iLO 2. Elles permettent de vérifier les contextes de recherche objet et utilisateur de la carte iLO 2.

2. Entrez également un nom d'utilisateur et un mot de passe tests. En général, on utilise un compte destiné à accéder à la carte iLO 2 testée. Il peut s'agir du même compte que l'administrateur d'annuaire. Toutefois, les tests ne permettent pas de vérifier l'authentification de l'utilisateur avec un compte « superutilisateur ». Ces données ne sont pas enregistrées par la carte iLO 2.

3. Cliquez sur **Start Test** (Démarrer test). Plusieurs tests sont lancés en arrière-plan, du ping réseau de l'utilisateur de l'annuaire à l'établissement d'une connexion SSL au serveur, en passant par l'évaluation des privilèges utilisateur tels qu'ils seraient contrôlés lors d'une connexion normale.

Pendant l'exécution des tests, la page est rafraîchie à intervalles réguliers. Pendant l'exécution du test, vous pouvez à tout moment arrêter le test ou rafraîchir la page manuellement. Consultez le lien d'aide sur la page pour obtenir des informations sur les tests et les actions à prendre en cas de problèmes.

Encryption (Codage)

iLO 2 dispose d'une sécurité performante concernant la supervision distante des environnements IT distribués. Les données du navigateur Web sont protégées par un codage SSL. Le codage SSL permet aux données HTTP de circuler sur le réseau de manière sécurisée. ILO 2 prend en charge les deux systèmes de codage les plus performants : Advanced Encryption Standard (AES) et Triple Data Encryption Standard (3DES). Les codages suivants sont pris en charge :

- AES 256 bits avec RSA, DHE et un MAC SHA1
- AES 256 bits avec RSA et un MAC SHA1
- AES 128 bits avec RSA, DHE et un MAC SHA1
- AES 128 bits avec RSA et un MAC SHA1
- Triple DES 168 bits avec RSA et un MAC SHA1
- Triple DES 168 bits avec RSA, DHE et un MAC SHA1

À l'aide d'un port SSH, iLO 2 dispose d'un codage performant pour les transactions CLP. Il prend également en charge les codages AES128-CBC et 3DES-CBC.

iLO 2 met en œuvre ces codages performants (AES et 3DES) sur des canaux sécurisés, y compris les transmissions HTTP sécurisées sur le navigateur, les ports SSH et XML. Si le codage AES/3DES est activé, vous devez utiliser une capacité de codage égale ou supérieure à ces codages pour vous connecter à iLO 2 via des canaux sécurisés. Les communications et les connexions sur des canaux moins sécurisés (un port Telnet par exemple) ne sont pas concernées par ce paramètre de codage AES/3DES.

Par défaut, les données de la console distante utilisent un codage bidirectionnel RC4 128 bits. L'utilitaire CPQLOCFG utilise un codage Triple DES 168 bits avec RSA et un MAC SHA1 pour envoyer de manière sécurisée les scripts RIBCL à iLO 2 via le réseau.

Paramètres de codage

Vous pouvez afficher ou modifier les paramètres de codage en cours à l'aide de l'interface CLP ou RIBCL d'iLO 2.

Pour ce faire, procédez comme suit :

1. Cliquez sur **Administration>Security>Encryption** (Administration>Sécurité>Codage).

   La page Encryption (Cryptage) comportant les paramètres de cryptage (codage négocié et application du cryptage) de iLO 2 s'affiche.

   - Current Negotiated Cipher (Codage négocié en cours) affiche le codage utilisé lors de la session du navigateur en cours. Une fois connecté à iLO 2 via le navigateur, ce dernier et iLO 2 négocient un paramètre de codage à utiliser lors de la session. La zone Current Negotiated Cipher (Codage négocié en cours) de la page Encryption (Cryptage) affiche le codage négocié.

     Encryption Enforcement Settings (Paramètres d'application du cryptage) affiche le cryptage en cours d'iLO 2. Enforce AES/3DES Encryption (Appliquer cryptage AES/3DES)(si activé) permet à iLO d'accepter uniquement les connexions via le navigateur et l'interface SSH correspondant à la capacité de codage minimale. Si ce paramètre est activé, une capacité de

codage comparable à AES ou 3DES doit être utilisée pour se connecter à iLO 2. Le paramètre Enforce AES/3DES Encryption (Appliquer cryptage AES/3DES) peut être activé ou désactivé.

2. Pour enregistrer les modifications, cliquez sur **Apply** (Appliquer).

   Si le paramètre Enforcement (Application) est activé, fermez tous les navigateurs après avoir cliqué sur **Apply** (Appliquer). Tout navigateur restant ouvert doit continuer d'utiliser un autre codage que AES/3DES.

Pour afficher ou modifier les paramètres de codage en cours via CLP ou RIBCL, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Connexion à iLO 2 à l'aide d'un cryptage AES/3DES

Après avoir activé le paramètre Enforce AES/3DES Encryption (Appliquer cryptage AES/3DES), iLO 2 requiert une connexion via des canaux sécurisés (navigateur Web, port SSH ou XML) à l'aide d'une capacité de codage comparable à AES ou 3DES.

Pour se connecter à iLO 2 via un navigateur, ce dernier doit être configuré avec une capacité de codage comparable à AES ou 3DES. Si le navigateur Web n'utilise pas les codages AES ou 3DES, iLO 2 affiche un message d'erreur demandant à l'utilisateur de fermer la connexion en cours et de sélectionner un codage approprié.

Pour ce faire, reportez-vous à la documentation de votre navigateur. Chaque navigateur dispose de sa propre méthode de sélection d'un codage négocié. Avant de modifier la capacité de codage du navigateur, vous devez vous déconnecter de iLO 2 au travers du navigateur en cours. Toute modification effectuée au niveau du paramètre de codage du navigateur lorsque vous êtes toujours connecté à iLO 2, peut entraîner l'utilisation d'un codage autre que AES/3DES.

Tous les navigateurs et systèmes d'exploitation client pris en charge par iLO 2 disposent de la fonction iLO 2 AES/3DES Encryption (Cryptage AES/3DES iLO 2) sauf dans le cas d'une utilisation de Windows 2000 Professionnel avec Internet Explorer. Par défaut, Windows 2000 Professionnel ne prend pas en charge les codages AES ou 3DES. Si un client utilise Windows® 2000 Professionnel, vous devez utiliser un autre navigateur ou mettre à jour le système d'exploitation.

Internet Explorer ne dispose pas d'un paramètre de capacité de codage sélectionnable par l'utilisateur. Vous devez modifier le registre pour permettre à Internet Explorer de se connecter à iLO 2 lorsque le paramètre Enforce AES/3DES Encryption (Appliquer cryptage AES/3DES) est activé. Pour ce faire, ouvrez le registre et définissez sur 1 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy`.

REMARQUE : la modification incorrecte du registre peut gravement endommager votre système. HP vous recommande de créer une copie de sauvegarde de toutes les données importantes contenues sur l'ordinateur avant de modifier le registre. Pour plus d'informations sur la manière de restaurer votre registre, reportez-vous à l'article de la base de connaissances Microsoft (http://support.microsoft.com/kb/307545).

Pour vous connecter à iLO 2 via une connexion SSH, reportez-vous à la documentation de l'utilitaire SSH pour définir la capacité de codage.

Lors d'une connexion via un canal XML, l'utilitaire CPQLOCFG utilise un codage 3DES sécurisé par défaut. Au niveau de la sortie XML, CPQLOCFG 2.26 ou version ultérieure affiche la capacité de codage de la connexion en cours suivante : Par exemple :

```
Connecting to Server..
Negotiated cipher: 168-bit Triple DES with RSA and a SHA1 MAC
```

Le cryptage AES n'est pas pris en charge par Internet Explorer sur un client Windows® 2000 Professionnel. Pour utiliser le cryptage AES avec ce système d'exploitation, utilisez un autre navigateur (Mozilla par exemple).

HP SIM single sign-on (Authentification unique HP SIM) (SSO)

HP SIM SSO vous permet de passer directement de HP SIM au processeur LOM sans étape de connexion intermédiaire. Pour utiliser SSO, une version à jour de HP SIM est requise. Vous devez également configurer le processeur LOM pour qu'il accepte les liens de HP SIM. Pour fonctionner correctement, HP SIM requiert les dernières mises à jour et derniers patches. Pour plus d'informations concernant HP Systems Insight Manager et les mises à jour disponibles, consultez le site Web HP (http://www.hp.com/go/hpsim).

HP SIM SSO est une fonctionnalité sous licence disponible lors de l'achat des licences en option. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21).

La page HP SIM SSO permet de visualiser et de configurer les paramètres SSO via l'interface iLO 2. Pour plus d'informations, reportez-vous à la section « Configuration de HP SIM SSO » (Configuration de HP SIM SSO à la page 60).

Pour accéder aux paramètres de configuration de HP SIM SSO, vous pouvez utiliser des scripts, des fichiers texte et une ligne de commande utilisant des clients texte tels que SSH sur un réseau ou à partir du système d'exploitation de l'ordinateur hôte. Les scripts SSO permettent d'utiliser les mêmes paramètres SSO sur tous les processeurs LOM. Pour plus d'informations sur les extensions CLP pour lire, modifier et écrire des paramètres de configuration HP SIM SSO et pour des exemples de scripts, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Configuration de iLO 2 pour HP SIM SSO

Avant de configurer SSO, vous devez disposer de l'adresse réseau de HP SIM et vérifier que la clé de licence est installée. Pour configurer SSO, procédez comme suit :

1. Activez l'option Single Sign-On Trust Mode (Mode Sécuriser authentification unique) en sélectionnant **Trust by Certificate** (Sécuriser par certificat) (recommandé), **Trust by Name** (Sécuriser par nom) ou **Trust All** (Agréer tout).
2. Ajoutez le certificat HP SIM du serveur à iLO 2.
   a. Cliquez sur **Add an HP SIM Server** (Ajouter un serveur HP SIM).
   b. Entrez l'adresse réseau du serveur HP SIM.
   c. Cliquez sur **Import Certificate** (Importer certificat).

      Le dépôt des certificats est fait pour autoriser cinq certificats iLO 2 standard. Cependant, les tailles des certificats peuvent changer si les certificats standard ne sont pas émis. 6 Ko de stockage associés sont attribués aux certificats et aux noms des serveurs iLO 2. Une fois cette capacité atteinte, plus aucun import n'est accepté.

Une fois l'authentification SSO configurée dans iLO 2, connectez-vous à HP SIM, localisez le processeur LOM, puis sélectionnez **Tools>System Information>iLO as...** (Outils>Informations système>iLO en tant que). HP SIM lance un nouveau navigateur connecté au processeur de supervision LOM.

Ajout de serveurs agréés HP SIM

Vous pouvez installer le serveur HP SIM à l'aide de script convenant à un déploiement massif. Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de*

commande du processeur de supervision HP Integrated Lights-Out. Pour ajouter les enregistrements du serveur HP SIM à l'aide du navigateur, procédez comme suit :

1. Cliquez sur **Administration>Security>HP SIM SSO** (Administration>Sécurité>HP SIM SSO).
2. Cliquez sur **Add an HP SIM Server** (Ajouter un serveur HP SIM).
3. Pour authentifier le serveur, effectuez l'une des procédures suivantes :
   - Pour ajouter un serveur HP SIM à l'aide de l'authentification Trust by Name (Sécuriser par nom), entrez son nom de réseau complet dans la section Add a Trusted HP SIM Server Name (Ajouter un nom de serveur HP SIM agréé). Cliquez sur **Add Server Name** (Ajouter un nom de serveur).

     Cette authentification utilise les noms de domaines complets. Par exemple : sim-host.hp.com au lieu de sim-host. Si vous n'êtes pas certain du nom de domaine complet, utilisez la commande `nslookup host`.
   - Pour rechercher et importer un certificat d'un serveur HP SIM agréé, entrez le nom de réseau complet du serveur HP SIM Server à la section Retrieve and import a certificate from a trusted HP SIM Server (Rechercher et importer un certificat d'un serveur HP SIM agréé). Cliquez sur **Import Certificate** (Importer certificat) pour demander le certificat au serveur HP SIM et l'importer automatiquement. Cet enregistrement prend en charge SSO Trust by Name (Sécuriser SSO par nom) et SSO Trust by Certificate (Sécuriser SSO par certificat).

     Pour éviter toute altération du certificat, importez directement un certificat du serveur HP SIM. Pour ce faire, recherchez la date du certificat HP SIM à l'aide des options suivantes :
     - À l'aide d'une fenêtre du navigateur différente, ouvrez le serveur HP SIM à l'aide de l'URL :

       ```
       http://<sim network address>:280/GetCertificate
       ```

       Coupez et collez les données du certificat de HP SIM dans iLO 2.
     - Exportez le certificat du serveur HP SIM depuis l'interface utilisateur de HP SIM en sélectionnant **Options>Security>Certificates>Server Certificate** (Options>Sécurité>Certificats>Certificat du serveur). Ouvrez le fichier à l'aide d'un éditeur de texte. Copiez et collez toutes les données brutes du certificat dans iLO 2.
     - À l'aide de lignes de commande sur le serveur HP SIM, le certificat est extrait via l'alias tomcat. Par exemple :

       ```
       mxcert -l tomcat
       ```

       Aperçu des données du certificat :

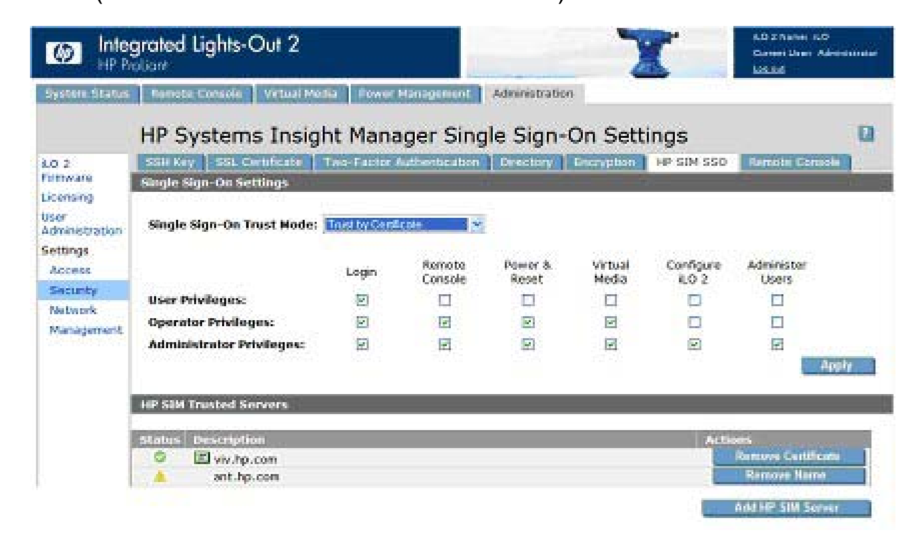
       ```
       -----BEGIN CERTIFICATE-----
       several lines of encoded data
       -----END CERTIFICATE-----
       ```

     Après avoir collé les données du certificat x.509 codé base 64 dans la section Directly import a HP SIM Server Certificate (Importer directement un certificat du serveur HP SIM), cliquez sur **Import Certificate** (Importer certificat) pour enregistrer les données. Ce type d'enregistrement prend en charge SSO Trust by Name (Sécuriser SSO par nom) et SSO Trust by Certificate (Sécuriser SSO par certificat).

D'autres moyens existent pour rechercher les données de certificat du serveur HP SIM. Pour plus d'informations, reportez-vous à la documentation de HP SIM.

Configuration de HP SIM SSO

La page HP SIM permet d'afficher et de configurer les paramètres de iLO 2 Single Sign-On (Authentification unique iLO2). Vous devez disposer du droit de configuration de iLO pour modifier ces paramètres. Pour accéder aux paramètres SSO d'iLO 2, cliquez sur **Administration>Security>HP SIM SSO** (Administration>Sécurité>HP SIM SSO).



La page HP Systems Insight Manager Single Sign-On Settings (Paramètres d'authentification unique de HP Systems Insight Manager) dispose des champs et options suivants :

- Single Sign-On Trust Mode (Mode Sécuriser authentification unique) : permet de contrôler l'acceptation des connexions initiées par SSO :
  - Trust None (Aucun agrément) (par défaut) : rejette toutes les demandes de connexion SSO.
  - Trust by Certificate (Sécuriser par certificat) (le plus sécurisé) : autorise uniquement les connexions SSO d'un serveur HP SIM correspondant au certificat précédemment importé dans iLO 2.
  - Trust by Name (Sécuriser par nom) : autorise les connexions SSO d'un serveur HP SIM correspondant au nom DNS ou au certificat précédemment importé dans iLO 2.
  - Trust All (Agréer tout) (le moins sécurisé) : accepte toutes les connexions SSO d'un serveur HP SIM.

    Les utilisateurs se connectant à HP SIM sont autorisés en fonction de l'affectation des rôles au niveau du serveur. L'affectation des rôles passe au processeur LOM lorsque SSO est tenté. Vous pouvez configurer des privilèges iLO 2 pour chaque rôle dans la section Single Sign-On Settings (Paramètres de l'authentification unique). Pour plus d'informations sur chacun des privilèges, reportez-vous à la section « Administration des utilisateurs » (Administration des utilisateurs à la page 24).

    À l'aide des comptes utilisateur basés sur les annuaires, SSO essaie de recevoir uniquement les privilèges affectés à cette section. Les paramètres de l'annuaire Lights-Out ne s'appliquent pas. Les affectations des privilèges par défaut sont :
  - User : Login only (Connexion utilisateur uniquement)

    - Operator (Opérateur) : Login (Connexion), Remote Console (Console distante), Power and Reset (Alimentation et réinitialisation) et Virtual Media (Support virtuel).
    - Administrator (Administrateur) : Login (Connexion), Remote Console (Console distante), Power and Reset (Alimentation et réinitialisation) et Virtual Media (Support virtuel), Configure iLO 2 (Configurer iLO 2) et Administer Users (Administrer les utilisateurs).
- HP SIM Trusted Servers (Serveurs agréés HP SIM) : permet d'afficher l'état des serveurs HP SIM agréés configurés pour utiliser SSO avec le processeur LOM en cours. Cliquez sur **Add a SIM Server** (Ajouter un serveur SIM) pour ajouter un nom de serveur, importer un certificat de serveur ou installer directement un certificat de serveur. Pour plus d'informations, reportez-vous à la section « Ajout de serveurs agréés HP SIM » (Ajout de serveurs agréés HP SIM à la page 58).

  Le tableau du serveur affiche une liste de serveurs HP SIM enregistrés ainsi que l'état de chacun. Le nombre actuel de systèmes autorisés est fonction de la taille des données de certificat stockées.

  Même si un système est enregistré, SSO peut être refusé à cause du niveau de sécurité en cours ou de l'état du certificat. Par exemple, si le nom du serveur HP SIM est enregistré et que le niveau de sécurité est défini sur Trust by Certificate (Sécuriser par certificat), SSO n'est pas autorisé de ce serveur. De la même manière, si un certificat de serveur HP SIM est importé mais que celui-ci a expiré, SSO n'est pas autorisé de ce serveur. De plus, les enregistrements ne sont pas autorisés lorsque SSO est désactivé. iLO 2 n'applique pas la révocation de certificat de serveur SSO.
    - Status (État) : indique l'état de l'enregistrement (s'il y en a d'installé).
    - Description : affiche le nom du serveur (ou l'objet du certificat). Une vignette sur un certificat indique que l'enregistrement contient un certificat stocké.
    - Actions : affiche les actions que vous pouvez réaliser sur un enregistrement sélectionné. Les actions affichées sont fonction du type et du nombre d'enregistrements installés :

      — Remove Name (Supprimer nom) : supprime l'enregistrement du nom de serveur.

      — Remove Certificate (Supprimer certificat) : supprime l'enregistrement du certificat.

Remote Console Computer Lock (Verrou d'ordinateur de console distante)

La fonction Remote Console Computer Lock (Verrou d'ordinateur de console distante) améliore la sécurité d'un serveur supervisé par iLO 2 en verrouillant automatiquement un système d'exploitation ou en déconnectant un utilisateur à la fin d'une session de console distante ou encore lors de la perte d'une liaison réseau à iLO 2. Contrairement à la console distante ou à la console distante intégrée, cette fonction est standard et ne nécessite pas de licence supplémentaire. Il en résulte que, si vous ouvrez une fenêtre de session de console distante ou de console distante intégrée et que cette fonction est configurée, elle verrouille le système d'exploitation lorsque la fenêtre est fermée, même si des licences de fonctions supplémentaires ne sont pas installées.

Vous pouvez afficher et configurer le paramètre Remote Console Computer Lock (Verrou d'ordinateur de console distante) à l'aide des onglets Administration ou Remote Console (Console distante) de l'interface iLO 2. Cette fonction est désactivée par défaut.

Pour modifier les paramètres Remote Console Computer Lock :

1. Connectez-vous à la carte iLO 2 en utilisant un compte doté du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2).

2. Cliquez sur **Administration>Security>Remote Console** (Administration>Sécurité>Console distante). La page correspondante s'affiche.



3. Modifiez les paramètres suivant les besoins :

   ◦ Windows - Utilisez cette option pour configurer iLO 2 afin de verrouiller un serveur supervisé exécuté sous un système d'exploitation Windows®. Le serveur affiche automatiquement la boîte de dialogue Computer Locked (Ordinateur verrouillé) lorsqu'une session de console distante est terminée ou que la liaison réseau à iLO 2 est perdue.

   ◦ Custom (Personnalisé) - Utilisez cette option pour configurer iLO 2 afin d'utiliser une clé personnalisée pour verrouiller un serveur supervisé ou pour déconnecter un utilisateur sur ce serveur. Vous pouvez sélectionner jusqu'à cinq clés dans la liste. La séquence de clés sélectionnées est automatiquement envoyée au système d'exploitation du serveur lorsqu'une session de console distante est terminée ou que la liaison réseau à iLO 2 est perdue.

   ◦ Disabled (Désactivé) - Utilisez cette option pour désactiver la fonction Remote Console Computer Lock. La fin d'une session de console distante ou la perte d'une liaison réseau à iLO 2 ne verrouille pas le serveur supervisé.

   Vous pouvez créer une séquence de clés Remote Console Computer Lock en utilisant les clés répertoriées dans le tableau suivant .

ESC	F4	1	e
L_ALT	F5	2	f
R_ALT	F6	3	g
L_SHIFT (L_MAJ)	F7	4	h
R_SHIFT (R_MAJ)	F8	5	i
L-CTRL	F9	6	j
R_CTRL	F10	7	k
L_GUI	F11	8	l
R_GUI	F12	9	m
INS (INSER)	" " (Espace)	:	n
DEL (SUPPR)	!	;	o
HOME (ORIGINE)	"	<	p
END (Fin)	#	=	q
PG_UP	$	>	r
PG_DN	%	?	s
ENTER (ENTRÉE)	&	@	t
TAB	'	[	u
BREAK	(	\	v

BACKSPACE (RETOUR ARRIÈRE)	)	]	w
NUM PLUS	*	^	x
NUM MINUS	+	_	y
SCRL LCK (ARRÊT DÉFIL)	,	'	z
SYS RQ	-	a	{
F1	.	b	}
F2	/	c	|
F3	0	d	~

4. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Cette fonction peut également être configurée en utilisant des scripts ou des lignes de commande. Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Réseau

Les onglets Network Settings (Paramètres réseau) et DCHP/DNS de la section Network (Réseau) permettent d'afficher et de modifier les paramètres réseau de iLO 2.

seuls les utilisateurs dotés du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2) sont autorisés à modifier ces paramètres. Les autres utilisateurs ne peuvent que consulter les paramètres qui ont été attribués.

Pour modifier les paramètres réseau de la carte iLO 2, procédez comme suit :

1. Connectez-vous à la carte iLO 2 en utilisant un compte doté du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2). Cliquez sur **Administration>Network** (Administration>Réseau).
2. Sélectionnez **Network Settings** (Paramètres réseau) ou **DHCP/DNS**.
3. Modifiez les paramètres selon vos besoins.
4. Ceci fait, cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

iLO 2 redémarre et la connexion de votre navigateur à iLO 2 est coupée. Pour rétablir la connexion, patientez 60 secondes avant de lancer une autre session de votre navigateur et de vous connecter.

Network Settings (Paramètres réseau)

La page Network Settings (Paramètres réseau) affiche l'adresse IP, le masque de sous-réseau et autres informations et paramètres TCP/IP relatifs à la carte réseau. L'écran Network Settings (Paramètres réseau) permet d'activer ou de désactiver DHCP et, pour les serveurs qui n'utilisent pas DHCP, de configurer une adresse IP statique. Tous les utilisateurs peuvent consulter les paramètres réseau, mais seuls ceux disposant du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2) peuvent les modifier. Pour accéder à la page Network Settings (Paramètres réseau), cliquez sur

Administration>Network>Network (Administration>Réseau>Réseau). La page Network Settings (Paramètres réseau) s'affiche avec les informations et paramètres ci-après :

- Le paramètre NIC (Carte réseau) permet d'affecter le mode Enabled (Activé), Disabled (Désactivé) ou Shared Network Port (Port réseau partagé) à la carte réseau iLO 2.
  - Enabled—Active l'interface réseau principale iLO 2.
  - Disabled—Désactive l'interface réseau iLO 2. Vous devez utiliser le RBSU iLO 2 ou tout autre utilitaire de script orienté hôte en vue de réactiver l'interface réseau.
  - Shared Network Port—Permet d'établir la mise en réseau grâce au port Ethernet hôte indiqué. Le port apparaît sur le réseau sous la forme de deux adresses distinctes (Ethernet MAC et IP). Pour plus d'informations, reportez-vous à la section « Port réseau partagé iLO 2 » (Port réseau partagé iLO 2 à la page 65).
- DHCP vous permet de sélectionner une adresse IP statique (désactivée) ou d'activer l'utilisation d'un serveur DHCP pour obtenir une adresse IP pour le sous-système iLO 2.

  Vous ne pouvez pas définir l'adresse IP et le masque de sous-réseau de la carte iLO 2 si DHCP est activé. La désactivation de DHCP permet de configurer l'adresse IP. Le champ IP Address (Adresse IP) apparaît également sur la page des paramètres DHCP/DNS à des fins pratiques. La modification de la valeur sur l'une des pages entraîne la modification du paramètre DHCP.
- IP Address (Adresse IP) correspond à l'adresse IP iLO 2. Si vous utilisez le DHCP, l'adresse IP iLO 2 est automatiquement fournie. Sinon, saisissez une adresse IP statique. Le champ IP Address (Adresse IP) apparaît sur la page des paramètres DHCP/DNS à des fins pratiques. Le fait de saisir des valeurs dans ce champ, dans l'une ou l'autre page, modifie l'adresse IP de la carte iLO 2.
- Subnet Mask (Masque de sous-réseau) désigne le masque de sous-réseau du réseau IP de la carte iLO 2. Si DHCP est en cours d'utilisation, le masque de sous-réseau est fourni automatiquement. Si tel n'est pas le cas, saisissez le masque de sous-réseau pour le réseau.
- Gateway IP Address (Adresse IP de passerelle) affiche l'adresse IP de la passerelle du réseau. Si vous utilisez le DHCP, l'adresse IP de la passerelle est automatiquement fournie. Dans le cas contraire, entrez-la.
- iLO 2 Subsystem Name (Nom du sous-système iLO 2) est un nom utilisé par le sous-système iLO 2. Si les paramètres DHCP et DNS sont correctement configurés, ce nom peut remplacer l'adresse IP pour établir la connexion au sous-système iLO 2. Pour plus d'informations, reportez-vous à la section « Limites relatives au nom du sous-système iLO 2 » (Limites relatives au nom du sous-système iLO 2 à la page 65).
- Link (Liaison) contrôle la vitesse et le mode duplex de l'émetteur-récepteur de réseau iLO 2. La vitesse de liaison de la carte principale iLO 2 dédiée peut être mise en évidence. Les paramètres Links (Liaisons) incluent les éléments suivants :
  - Automatic (Automatique) (par défaut) permet à la carte iLO 2 de négocier la vitesse de liaison la plus élevée possible et le mode duplex lors d'une connexion au réseau.
  - 100Mb/FD (100 Mo/FD) force une connexion 100 Mo en full duplex.
  - 100Mb/HD (100 Mo/HD) force une connexion 100 Mo en half duplex.
  - 10Mb/FD (10 Mo/FD) force une connexion 10 Mo en full duplex.
  - 10Mb/HD (10 Mo/HD) force une connexion 10 Mo en half duplex.

    Si la détection automatique est désactivée, le commutateur de réseau doit correspondre aux paramètres iLO 2 pour prévenir des problèmes d'accès à iLO 2.

Limites relatives au nom du sous-système iLO 2

Le nom du sous-système iLO 2 correspond au nom DNS du sous-système iLO 2. Par exemple, `ilo` au lieu de `ilo.hp.com`. À condition que les paramètres DHCP et DNS soient correctement configurés, ce nom peut remplacer l'adresse IP pour établir la connexion au sous-système iLO 2.

- Limites relatives au service d'attribution de noms : le nom du sous-système fait partie du nom DNS et du nom WINS. Cependant, les limites relatives au DNS et au WINS sont différentes :
  - Le DNS permet l'utilisation de caractères alphanumériques et de tirets. Le WINS permet l'utilisation de caractères alphanumériques, de tirets et de traits de soulignement.
  - Les noms de sous-systèmes WINS sont tronqués après 15 caractères, tandis que les noms des sous-systèmes DNS ne le sont pas.

    Si vous avez besoin d'utiliser des traits de soulignement, vous pouvez les entrer dans l'utilitaire RBSU ou à l'aide de l'utilitaire de génération de scripts iLO 2.

    REMARQUE : les limites relatives au service d'attribution de noms s'appliquent également au nom de domaine.

    Pour éviter les problèmes d'espace dans les noms :
  - N'utilisez pas le trait de soulignement.
  - Limitez les noms des sous-systèmes à 15 caractères.
  - Assurez-vous de pouvoir tester iLO (ping) par son adresse IP et par son nom DNS/WINS.
  - Assurez-vous que NSLOOKUP résolve correctement l'adresse réseau de iLO et qu'il n'existe aucun conflit lié à l'existence d'espace dans les noms.
  - Assurez-vous que le DNS et le WINS résolvent correctement le nom tous les deux (si vous les utilisez tous les deux).
  - Videz le nom DNS lorsque vous effectuez des modifications sur les espaces dans les noms.

Port réseau partagé iLO 2

La fonction iLO 2 Shared Network Port (Port réseau partagé iLO 2) permet de choisir la carte réseau système ou la carte réseau de supervision iLO 2 dédiée pour la gestion du serveur. Lorsque vous activez le port réseau partagé iLO 2, le trafic réseau standard ainsi que le trafic réseau dédié à l'iLO 2 passent via la carte réseau système.

iLO 2 est compatible avec les serveurs qui ne comportent pas forcément une carte réseau de supervision dédiée iLO 2. Sur les serveurs utilisant une carte réseau de supervision dédiée iLO 2, la configuration matérielle standard prévoit une connectivité réseau iLO 2 via le port réseau partagé iLO 2 uniquement. iLO 2 détecte l'absence éventuelle d'une carte réseau de supervision dédiée iLO 2 et bascule automatiquement vers le port réseau partagé. Sur certains de ces serveurs, une carte réseau de supervision dédiée iLO 2 peut être ajoutée comme option matérielle. Si une carte réseau de supervision dédiée iLO 2 est disponible en tant qu'option matérielle, iLO 2 bascule par défaut vers cette carte. Sur les serveurs utilisant une carte réseau de supervision dédiée iLO 2, vous pouvez activer un fonctionnement de port réseau partagé via l'interface iLO 2.

Le port réseau partagé iLO 2 utilise le port réseau nommé NIC 1 sur le panneau arrière du serveur. La numérotation des cartes réseau dans le système d'exploitation peut différer de la numérotation système. Le port réseau partagé iLO 2 ne subit pas de dégradation de ses performances iLO 2. Le trafic maximal de iLO 2 est inférieur à 2 Mo (sur une carte réseau d'une vitesse de 1000 Mo). Le trafic moyen de iLO 2 est irrégulier et faible.

Le port réseau partagé n'est pas disponible sur les serveurs HP ProLiant ML310 G3, ML310 G4, BL20p G4 ni sur tous les serveurs lame c-Class.

Caractéristiques et limites du port de supervision partagé iLO 2

Le port réseau partagé iLO 2 et le port Carte réseau de supervision dédiée iLO 2) sont utilisés dans le cadre de la gestion de serveur iLO 2. À cet égard, vous ne pouvez utiliser que le port réseau partagé iLO 2 et la carte réseau de supervision dédiée iLO 2. Ils ne peuvent pas fonctionner simultanément. Si vous activez la carte réseau de supervision dédiée iLO 2, vous désactiverez le port réseau partagé iLO 2. Si vous activez le port réseau partagé iLO 2, vous désactiverez la carte réseau de supervision dédiée iLO 2.

Cependant, la désactivation du port réseau partagé ne désactive pas complètement la carte réseau système. Le trafic réseau régulier transite toujours par celle-ci. Lorsque le trafic réseau du port réseau partagé est désactivé, le trafic à destination ou en provenance de la carte iLO 2 ne transite pas sur celle-ci par le port réseau partagé car ce dernier n'est plus partagé avec iLO 2.

Le port réseau partagé ne doit pas être considéré comme une fonction de disponibilité. Il a pour but de permettre une consolidation des ports réseau gérés. L'utilisation de cette fonction peut créer une erreur. Ainsi, si le port est en échec ou s'il est débranché, l'hôte et iLO 2 deviennent tous les deux indisponibles sur le réseau.

Activation de la fonction iLO 2 Shared Network Port (Port réseau partagé iLO 2)

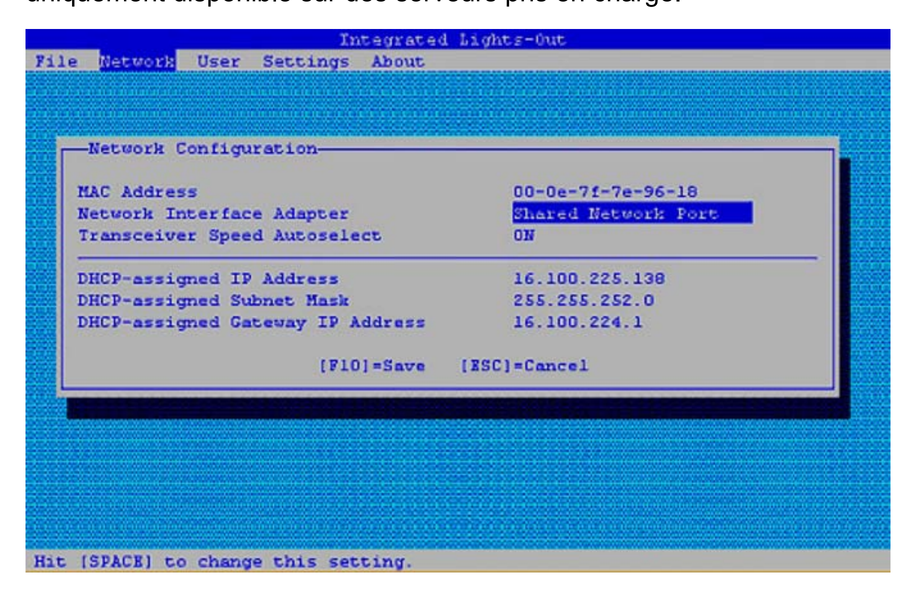
Par défaut, la fonction iLO 2 Shared Network Port (Port réseau partagé iLO 2) est désactivée. Elle peut être activée à l'aide des éléments suivants :

- iLO 2 RBSU
- Interface Web iLO 2
- Scripts XML

Activation de la fonction iLO 2 Shared Network Port (Port réseau partagé iLO 2) via iLO 2 RBSU

1. Connectez le port 1 de la carte réseau du serveur à un réseau LAN.
2. Lorsque vous y êtes invité pendant le test POST, appuyez sur la touche **F8** pour accéder à iLO 2 RBSU.
3. Sélectionnez **Network>NIC>TCP/IP** (Réseau>Carte réseau>TCP/IP), puis appuyez sur la touche **Entrée**.

4. Dans le menu Network Configuration (Configuration réseau), appuyez sur la barre d'espacement pour basculer le champ Network Interface Adapter (Adaptateur d'interface réseau) sur Shared Network Port (Port réseau partagé). L'option Shared Network Port (Port réseau partagé) est uniquement disponible sur des serveurs pris en charge.



5. Appuyez sur la touche **F10** pour enregistrer la configuration.

6. Sélectionnez **File>Exit** (Fichier>Quitter), puis appuyez sur la touche **Entrée**.

Après la réinitialisation de iLO 2, la fonction Shared Network Port (Port réseau partagé) est active. Tout trafic réseau à destination ou en provenance de iLO 2 est acheminé via le port 1 de la carte réseau du système.

Activation de la fonction iLO 2 Shared Network Port (Port réseau partagé iLO) à l'aide de l'interface Web

1. Connectez le port 1 de la carte réseau de iLO 2 à un réseau LAN.

2. Ouvrez un navigateur et accédez au nom DNS ou l'adresse IP de iLO 2.

3. Sélectionnez **Administration>Network Settings** (Administration>Paramètres réseau).

4. Dans la page Network Settings (Paramètres réseau), sélectionnez **Shared Network Port** (Port réseau partagé). La fonction Shared Network (Réseau partagé) est uniquement disponible sur les serveurs pris en charge.

5. Cliquez sur **Apply** (Appliquer) au bas de la page.

6. Cliquez sur **Yes** (Oui) dans la boîte de dialogue d'avertissement, puis sur **OK**.

Après la réinitialisation de iLO 2, la fonction Shared Network Port (Port réseau partagé) est active. Tout trafic réseau à destination ou en provenance de iLO 2 est acheminé via le port 1 de la carte réseau du système.

Seul le port Shared Network Port (Port partagé réseau) ou iLO 2 Dedicated Management NIC (Carte réseau de supervision dédiée iLO 2) est actif pour la supervision du serveur. Ils ne peuvent pas être activés simultanément.

Réactivation du port de supervision iLO 2 dédié

L'interface Web iLO 2, RBSU ou la génération de scripts XML (décrite dans le manuel de référence de génération de scripts et de lignes de commandes) doit être utilisé pour activer à nouveau iLO 2

Dedicated Management NIC (Carte réseau de supervision dédiée iLO 2). La réactivation d'iLO 2 à l'aide de RBSU requiert le redémarrage du système.

Pour réactiver iLO 2 Dedicated Management NIC (Carte de supervision dédiée iLO 2) à l'aide de RBSU :

1. Connectez le port de supervision de la carte réseau dédiée iLO 2 à un réseau LAN à partir duquel le serveur est géré.
2. Réamorcez le serveur.
3. Lorsque vous y êtes invité pendant le test POST, appuyez sur la touche **F8** pour accéder à iLO 2 RBSU.
4. Sélectionnez **Network>NIC>TCP/IP** (Réseau>Carte réseau>TCP/IP), puis appuyez sur la touche **Entrée**.
5. Dans le menu Network Configuration (Configuration réseau), appuyez sur la barre d'espacement pour basculer le champ Network Interface Adapter (Adaptateur d'interface réseau) sur ON (Activé).
6. Appuyez sur la touche **F10** pour enregistrer la configuration.
7. Sélectionnez **File>Exit** (Fichier>Quitter), puis appuyez sur la touche **Entrée**.

Une fois la réinitialisation de iLO 2 effectuée, le port iLO 2 Dedicated Management NIC (Carte réseau de supervision dédiée iLO 2) est actif.

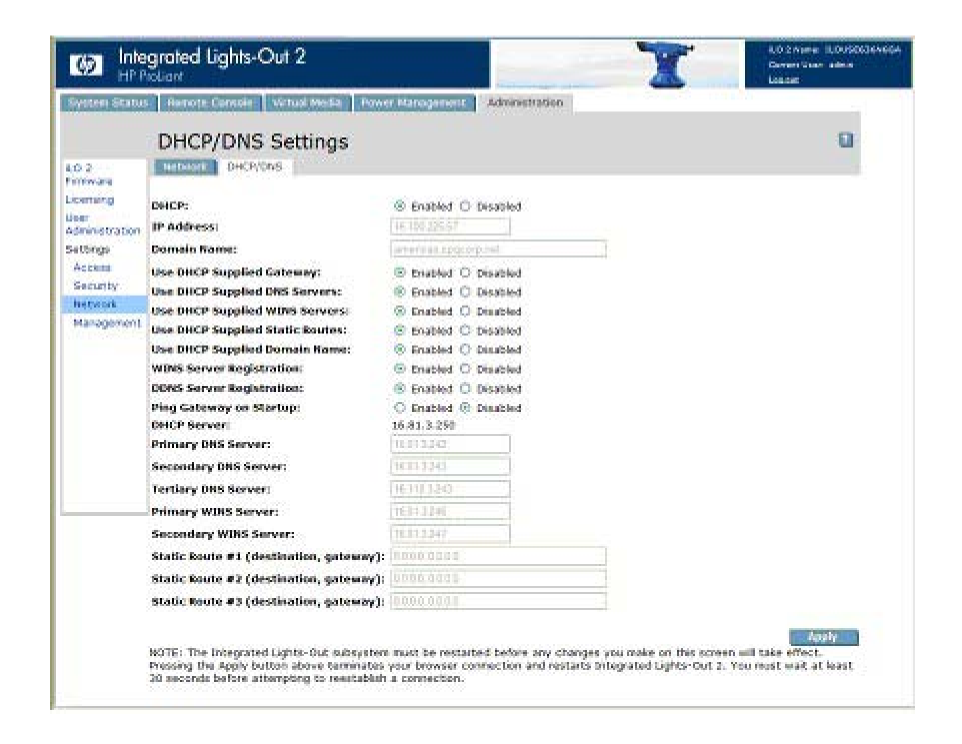
Pour réactiver iLO 2 Dedicated Management NIC (Carte réseau de supervision dédiée iLO 2) à l'aide de l'interface iLO 2 :

1. Ouvrez un navigateur et accédez au nom DNS ou à l'adresse IP iLO 2.
2. Dans la page Network Settings (Paramètres réseau), sélectionnez **Enabled** (Activé) pour la carte réseau iLO 2.
3. Cliquez sur **Apply** (Appliquer). Une boîte de dialogue d'avertissement apparaît.
4. Cliquez sur **Yes** (Oui), puis sur **OK**.

Une fois la réinitialisation de iLO 2 effectuée, le port iLO 2 Dedicated Management NIC (Carte réseau de supervision dédiée iLO 2) est actif. Lors de l'utilisation de IRC via le port iLO 2 Dedicated Management NIC (Carte réseau de supervision dédiée iLO 2) et en fonction du trafic réseau, vous risquez de manque de temps pour appuyer sur les touches RBSU lors du POST.

Paramètres DHCP/DNS

La page des paramètres DHCP/DNS iLO 2 contient les informations de configuration DHCP/DNS de iLO 2. Tous les utilisateurs peuvent afficher les paramètres DHCP/DNS, mais seulement ceux disposant du privilège Configure iLO 2 Settings (Configurer les paramètres iLO 2) peuvent les modifier. Il est également possible de modifier ces paramètres à l'aide de iLO 2 RBSU (F8 pendant le processus POST). Pour accéder aux paramètres DHCP/DNS, cliquez sur **Administration>Network>DHCP/DNS** (Administration>Réseau>DHCP/DNS). La page des paramètres DHCP/DNS s'affiche.



Les options suivantes sont disponibles :

- DHCP permet de sélectionner une adresse IP statique (désactivée) ou d'activer l'utilisation d'un serveur DHCP pour obtenir une adresse IP pour le sous-système iLO 2.

  Il est impossible de définir l'adresse IP iLO 2 si DHCP est activé. La désactivation de DHCP permet de configurer l'adresse IP. Le champ IP Address (Adresse IP) apparaît également sur la page Network Settings (Paramètres réseau) à des fins pratiques. La modification de la valeur sur l'une des pages entraîne la modification du paramètre DHCP.

- IP Address (Adresse IP) correspond à l'adresse IP iLO 2. Si vous utilisez le DHCP, l'adresse IP iLO 2 est automatiquement fournie. Sinon, saisissez une adresse IP statique. Le champ IP Address (Adresse IP) apparaît sur la page Network Settings (Paramètres réseau) à des fins pratiques. En modifiant la valeur sur une page, vous modifiez l'adresse IP de iLO 2.

- Domain Name (Nom de domaine) correspond au domaine sur lequel réside le sous-système iLO 2. Ce nom est attribué par DHCP (si DHCP est activé). L'activation de DHCP permet de configurer les options DHCP suivantes :

  - Use DHCP Supplied Gateway (Utiliser la passerelle fournie par DHCP) - Bascule si iLO 2 utilise la passerelle fournie par le serveur DHCP. Dans le cas contraire, entrez une adresse de passerelle dans la zone Gateway IP Address (Adresse IP passerelle).

  - Use DHCP Supplied DNS Servers (Utiliser les serveurs DNS fournis par DHCP) - Bascule si iLO 2 utilise la liste des serveurs DNS fournie par le serveur DHCP. Dans le cas contraire, entrez l'adresse du serveur DNS dans les champs Primary DNS Server (Serveur DNS primaire), Secondary DNS Server (Serveur DNS secondaire) et Tertiary DNS Server (Serveur DNS tertiaire).

  - Use DHCP Supplied WINS Servers (Utiliser les serveurs WINS fournis par DHCP) - Bascule si iLO 2 utilise la liste des serveurs WINS fournie par le serveur DHCP. Dans le cas contraire, entrez l'adresse du serveur WINS dans les champs Primary WINS Server (Serveur WINS primaire) et Secondary WINS Server (Serveur WINS secondaire).

    - Use DHCP Supplied Static Routes (Utiliser les routes statiques fournies par DHCP) - Bascule si iLO 2 utilise la route statique fournie par le serveur DHCP. Dans le cas contraire, entrez l'adresse de la route statique dans les champs Static Route #1 (Route statique n□‹1), Static Route #2 (Route statique n□‹2) ou Static Route #3 (Route statique n□‹3).
    - Use DHCP Supplied Domain Name (Utiliser le nom de domaine fourni par DHCP) - Bascule si iLO 2 utilise le nom de domaine fourni par le serveur DHCP. Dans le cas contraire, entrez un nom de domaine dans la zone Domain Name (Nom de domaine).
- WINS Server Registration (Enregistrement serveur WINS) - Bascule si iLO 2 enregistre son nom auprès d'un serveur WINS.
- DDNS Server Registration (Enregistrement serveur DDNS) - Bascule si iLO 2 enregistre son nom auprès d'un serveur DDNS.
- L'option Ping Gateway on Startup (Tester passerelle au démarrage) provoque l'envoi par iLO 2 de quatre paquets de requêtes d'écho ICMP à la passerelle lors de l'initialisation de iLO 2. Cette option permet de s'assurer que l'entrée de cache du protocole ARP est mise à jour sur le routeur responsable du routage des paquets de et vers iLO 2.
- DHCP Server (Serveur DHCP) est l'adresse IP du serveur DHCP. Ce champ ne peut pas être attribué. Il est reçu en provenance de DHCP si DHCP est activé et représente la dernière adresse connue valide du serveur DHCP.
- Primary DNS Server (Serveur DNS primaire), Secondary DNS Server (Serveur DNS secondaire) et Tertiary DNS Server (Serveur DNS tertiaire) sont les adresses IP des serveurs DNS. Si ces champs sont fournis par le serveur DHCP, ils sont automatiquement renseignés. Sinon, saisissez les adresses IP manuellement.
- Primary WINS Server (Serveur WINS primaire) et Secondary WINS Server (Serveur WINS secondaire) sont les adresses IP des serveurs WINS. Si ces champs sont fournis par le serveur DHCP, ils sont automatiquement renseignés. Sinon, saisissez les adresses IP manuellement.
- Static Route #1 (Route statique n° 1), Static Route #2 (Route statique n° 2) et Static Route #3 (Route statique n° 3) (destination, passerelle) sont les adresses de passerelle de destination du réseau. Entrez jusqu'à trois paires de routage destination/passerelle réseau.

Paramètres SNMP/Insight Manager

L'option Management (Supervision) de la section Administration affiche la page SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager). La page SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager) permet de configurer les alertes SNMP, de générer une alerte de test et de configurer l'intégration avec HP SIM.

Activation des alertes SNMP

iLO 2 prend en charge jusqu'à trois adresses IP pour la réception des alertes SNMP. En général, les adresses utilisées sont identiques à l'adresse IP de la console du serveur HP SIM.

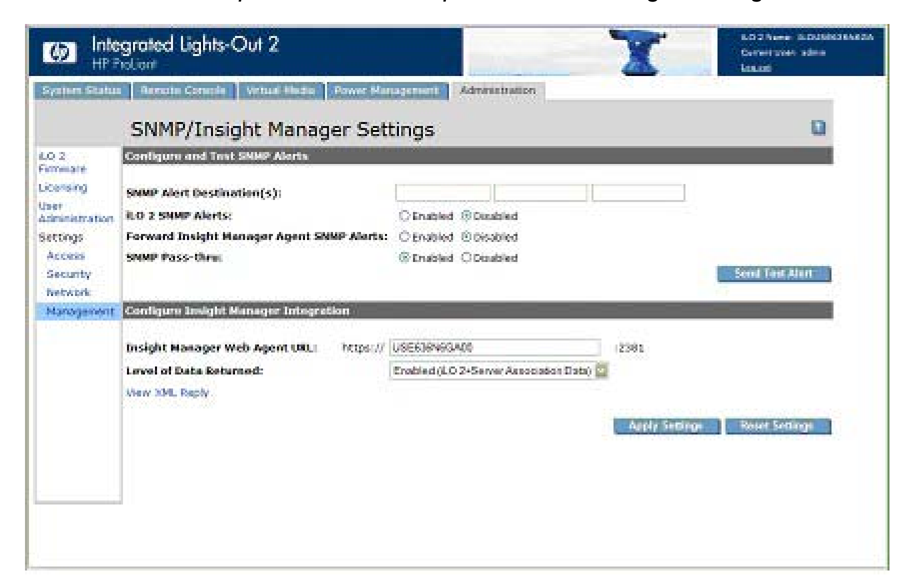
seuls les utilisateurs dotés du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2) sont autorisés à modifier ces paramètres. Les autres peuvent uniquement consulter les paramètres attribués.

Les options d'alerte suivantes sont disponibles dans l'écran SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager) :

- SNMP Alert Destination(s) (Destination(s) des alertes SNMP)
- iLO 2 SNMP Alerts (Alertes SNMP iLO 2)

- Forward Insight Manager Agent SNMP Alerts (Transmettre les alertes SNMP des agents Insight Manager)
- SNMP Pass-thru (Émulation SNMP)
- pClass Alert Fowarding (Transfert des alertes p-Class) (s'affiche sur les serveurs pClass uniquement)

Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.



Pour configurer les alertes :

1. Connectez-vous à la carte iLO 2 en utilisant un compte doté du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2).
2. Sélectionnez **Management** (Supervision) dans l'onglet Administration. L'écran SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager) apparaît.
3. Dans les champs SNMP Alert Destination(s) (Destination(s) des alertes SNMP), saisissez jusqu'à trois adresses IP, à partir desquelles vous recevrez les alertes SNMP, et sélectionnez les options d'alerte prises en charge par iLO 2.
4. Cliquez sur **Apply Settings** (Appliquer les paramètres).

Les alertes de test comprennent un trap Insight Manager SNMP (SNMP Insight Manager) et sont utilisées pour vérifier la connectivité du réseau iLO 2 sur HP SIM. Seuls les utilisateurs dotés du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2) peuvent envoyer des alertes de test.

Avant d'envoyer une alerte de test, vérifiez que les modifications apportées aux champs SNMP Alert Destination(s) (Destination(s) des alertes SNMP) ont été enregistrées.

Pour envoyer une alerte de test :

1. Sélectionnez **Management** (Supervision) dans l'onglet Administration. L'écran SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager) apparaît.
2. Cliquez sur **Send Test Alert** (Envoyer alerte de test) dans la section Configure and Test SNMP Alerts (Configurer et tester les alertes SNMP) pour générer une alerte de test et l'envoyer aux adresses TCP/IP enregistrées dans les champs SNMP Alert Destinations (Destinations des alertes SNMP).

3. Une fois l'alerte générée, un écran de confirmation s'affiche.
4. Vérifiez que le trap a bien été reçu sur la console HP SIM.

Définitions des traps générés par SNMP

Vous pouvez générer les traps SNMP suivants sur les serveurs BL c-Class et iLO 2 :

- ALERT_TEST permet de vérifier que la configuration SNMP, la console SNMP cliente et le réseau fonctionnent correctement. Vous pouvez utiliser l'interface iLO 2 pour générer cette alerte afin d'en vérifier la bonne réception au niveau de la console SNMP. Vous pouvez également générer cette alerte à l'aide de la ROM de l'option iLO 2 pour vérifier les paramètres de configuration SNMP.
- ALERT_SERVER_POWER se produit lorsque le processeur de supervision iLO 2 détecte une transition inopinée de l'alimentation du système hôte, de marche vers arrêt ou inversement. Les transitions de l'alimentation du système hôte sont inopinées lorsque le changement se produit à cause d'événements inconnus du processeur de supervision. Cette alerte n'est pas générée lorsque le système est mis sous tension ou hors tension à l'aide de l'interface iLO 2, de la fonction CLI, RIBCL ou une autre fonction de supervision. Si le serveur est mis hors tension à cause du système d'exploitation, de l'activation d'une touche d'alimentation physique ou de toute autre manière, l'alerte est générée et envoyée.
- ALERT_SERVER_RESET se produit lorsque le processeur de supervision iLO 2 est utilisé pour réaliser un redémarrage à froid ou à chaud du système hôte. Cette alerte est également envoyée lorsque le processeur de supervision iLO 2 détecte que le système hôte est en cours de réinitialisation à cause d'événements inconnus de ce même processeur. Certains comportements ou actions du système d'exploitation peuvent entraîner la détection de ce type d'événement, auquel cas l'alerte est transmise.
- ALERT_ILLEGAL_LOGIN est une alerte SNMP transmise lors d'une tentative de connexion à l'aide d'un nom d'utilisateur ou d'un mot de passe incorrect. Cette alerte est transmise quel que soit le type de connexion : interface Web, port série, Telnet, SSH ou RIBCL.
- ALERT_LOGS_FULL est une alerte SNMP transmise lorsque le journal des événements iLO 2 est complet et qu'il fait l'objet d'une tentative de consignation d'un nouvel événement.
- ALERT_SELFTEST_FAILURE est une alerte SNMP transmise lorsque iLO 2 détecte une erreur dans l'un des composants internes surveillés. En cas de détection d'erreur, une alerte est transmise.
- L'alerte ALERT_SECURITY_ENABLED est transmise lorsque le processeur de supervision iLO 2 détecte une transition du commutateur de neutralisation de la sécurité à l'état actif.
- L'alerte ALERT_SECURITY_DIABLED est transmise lorsque le processeur de supervision iLO 2 détecte une transition du commutateur de neutralisation de la sécurité à l'état inactif.
- L'alerte ALERT_HOST_GENERATED est générée lorsque le processeur de supervision iLO 2 a fait l'objet d'une demande de transmission d'une alerte hôte (passthrough SNMP) et qu'il n'a pu envoyer l'alerte SNMP d'origine. iLO 2 tente de transmettre cette alerte générique afin d'aviser la console de supervision SNMP qu'une alerte devant être envoyée par le système hôte a échoué.

Configuration de l'intégration avec Insight Manager

Le paramètre Insight Manager Web Agent URL (URL des agents Web Insight Manager) (nom DNS ou adresse IP) définit la cible du lien Insight Agent contenu dans les pages iLO 2. En général, ce lien est l'adresse IP ou le nom DNS de l'agent de supervision fonctionnant sur le système d'exploitation du serveur hôte.

Entrez l'adresse IP du serveur hôte. Le protocole (https://) et le numéro de port (:2381) sont automatiquement ajoutés à l'adresse IP ou au nom DNS pour autoriser l'accès aux agents Web Insight Management à partir de iLO 2.

Lorsque le paramètre Insight Manager Web Agent URL (URL des agents Web Insight Manager) a été défini à l'aide d'une autre méthode (par exemple, CPQLOCFG), cliquez sur le bouton Réactualiser du navigateur pour afficher l'URL mise à jour.

Le paramètre Level of Data Returned (Niveau de données retournées) contrôle le contenu d'un message de détection anonyme reçu par iLO 2. Les informations retournées sont utilisées pour les demandes d'identification HTTP Insight Manager. Les options suivantes sont disponibles :

- Enabled (Activé) (par défaut) permet à Insight Manager d'associer le processeur de supervision au serveur hôte et fournit des données suffisantes permettant l'intégration à HP SIM.
- Disabled (Désactivé) empêche iLO 2 de répondre aux demandes HP SIM.
- View XML Reply (Afficher réponse XML) permet d'analyser les données retournées aux paramètres.

  Affichez la réponse qui sera retournée à Insight Manager lorsqu'une demande d'identification du processeur de supervision est effectuée à l'aide de ce lien.

Pour enregistrer les modifications, cliquez sur **Apply Settings** (Appliquer paramètres). Cliquez sur **Reset Settings** (Réinitialiser paramètres) pour supprimer le contenu des champs et revenir à l'état précédent. Le bouton Reset Settings n'enregistre aucune modification.

Pour plus d'informations sur les agents Insight, cliquez sur **System Status>Insight Agent** (État du système>Agent Insight).

Configuration des serveurs ProLiant BL p-Class

Vous pouvez accéder aux serveurs ProLiant BL p-Class et les configurer à partir :

- du port de diagnostic iLO 2 à l'avant du serveur
- de l'« Installation basée sur le navigateur (Installation de iLO 2 à l'aide de l'option basée sur le navigateur à la page 14) », laquelle méthode permet de réaliser la configuration initiale du système via le port de diagnostic d'iLO 2
- de l'assistant d'installation détaillé via l'installation HP BladeSystem

Pour les serveurs lame p-Class installés dans des boîtiers dotés de fonds de panier de supervision mis à jour prenant en charge les serveurs lame haute densité, iLO 2 permet la configuration IP statique initiale du boîtier. La configuration initiale du compartiment 1 permet d'affecter des adresses IP prédéfinies à toutes les cartes iLO 2 qui seront installées ultérieurement dans le boîtier. Cette fonction est prise en charge dans les versions iLO 1.55 ou ultérieures.

Spécifications relatives aux utilisateurs de serveur ProLiant BL p-Class

- Les utilisateurs doivent disposer du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2).
- Une connexion réseau à iLO 2 doit être disponible et fonctionner correctement.

Configuration IP statique

La configuration IP statique est mise en œuvre à l'aide de l'option Static IP Bay Settings (Paramètres IP statique) de l'onglet BL p-Class. Cette option facilite le déploiement initial d'un boîtier entier ou le déploiement ultérieur des lames dans un boîtier existant. Même si la méthode préconisée pour

l'affectation d'adresses IP à chaque iLO 2 de chacun des serveurs lame consiste à utiliser DHCP et DNS, ces protocoles ne sont pas toujours disponibles sur d'autres réseaux que des réseaux de production.

Par exemple, après avoir configuré l'IP statique de la lame dans le compartiment 1, l'ajout ultérieur de lames dans le boîtier présuppose l'utilisation d'adresses sans DHCP. Les adresses réseau sont attribuées en fonction de la position des lames dans le compartiment 1 : 192.168.1.1, compartiment 2 : 192.168.1.2 et ainsi de suite. Le déploiement ultérieur de lames ne requiert pas de configuration supplémentaire et l'adresse réseau correspond au numéro du compartiment.

La configuration IP statique automatise la première étape du déploiement de lames BL p-Class, en activant le processeur de supervision iLO 2 dans chaque connecteur de lame afin d'obtenir une adresse IP prédéfinie sans utiliser DHCP. iLO 2 est immédiatement accessible pour le déploiement de serveurs à l'aide de Virtual Media (Support virtuel) et d'autres fonctions d'administration à distance.

La configuration IP statique utilise le mode d'adressage Static IP Bay Configuration (Configuration IP statique) qui permet d'affecter des adresses IP à chaque iLO 2 selon l'emplacement des connecteurs dans le boîtier des serveurs respectifs. En affectant un jeu d'adresses IP au boîtier, vous bénéficiez des avantages d'une configuration IP statique, sans qu'il soit nécessaire de configurer chaque iLO 2 localement.

La configuration IP statique de iLO 2 offre les avantages suivants :

- Pas de coûts associés à une infrastructure DHCP assurant la prise en charge de l'environnement de lames de serveur
- Configuration plus aisée avec génération automatique des adresses iLO 2 pour tout ou partie des compartiments sélectionnés

La configuration IP statique n'est pas prise en charge par les boîtiers de lame G1 BL. Pour afficher des informations sur un boîtier donné, cliquez sur **BL p-Class>Rack View>Details** (BL p-Class>Afficher rack>Détails). La configuration IP statique n'est pas prise en charge par les boîtiers lorsque le message `BL Enclosure G1` apparaît dans le champ Enclosure Type (Type de boîtier).

Lorsqu'une lame est à nouveau déployée, la configuration IP statique risque de ne pas se terminer comme prévu. Pour corriger cela, vérifiez que la lame utilise le microprogramme iLO 2 en cours, puis réinitialisez la configuration iLO 2 aux valeurs d'usine par défaut à l'aide de iLO 2 RBSU.

Configuration d'un boîtier de serveur lame ProLiant BL p-Class

Pour configurer un boîtier de serveur lame ProLiant BL p-Class à l'aide de l'adressage IP statique :

1. Installez une lame de serveur dans le compartiment n°1 du boîtier BL p-Class. Il n'est pas nécessaire de configurer la lame de serveur ou d'installer un système d'exploitation. La lame de serveur doit être configurée avant d'en installer d'autres dans le boîtier.
2. Connectez un client au port iLO 2 du panneau avant du serveur lame à l'aide du câble d'E/S local. Le câble d'E/S se connecte au port d'E/S situé sur la face avant du serveur lame. Cette connexion active l'adresse IP statique 192.168.1.1 pour l'interface Web iLO 2.
3. Configurez le paramètre de boîtier. À l'aide de l'interface Web iLO 2, sélectionnez l'onglet BL p-Class pour accéder aux paramètres IP statique du boîtier. L'onglet BL p-Class fournit une interface utilisateur permettant de configurer les adresses IP statiques au niveau du boîtier.
4. Sélectionnez une adresse de démarrage raisonnable, le ou les derniers chiffres correspondant au numéro de compartiment de chaque serveur lame (exemple : 192.168.100.1 à 192.168.100.16) afin de concevoir un système de numérotation facile à retenir.
5. Réinitialisez le compartiment n° 1, si nécessaire. Vous devez réinitialiser la lame du compartiment n° 1 uniquement si vous prévoyez d'utiliser une adresse Static IP Bay Configuration (Configuration

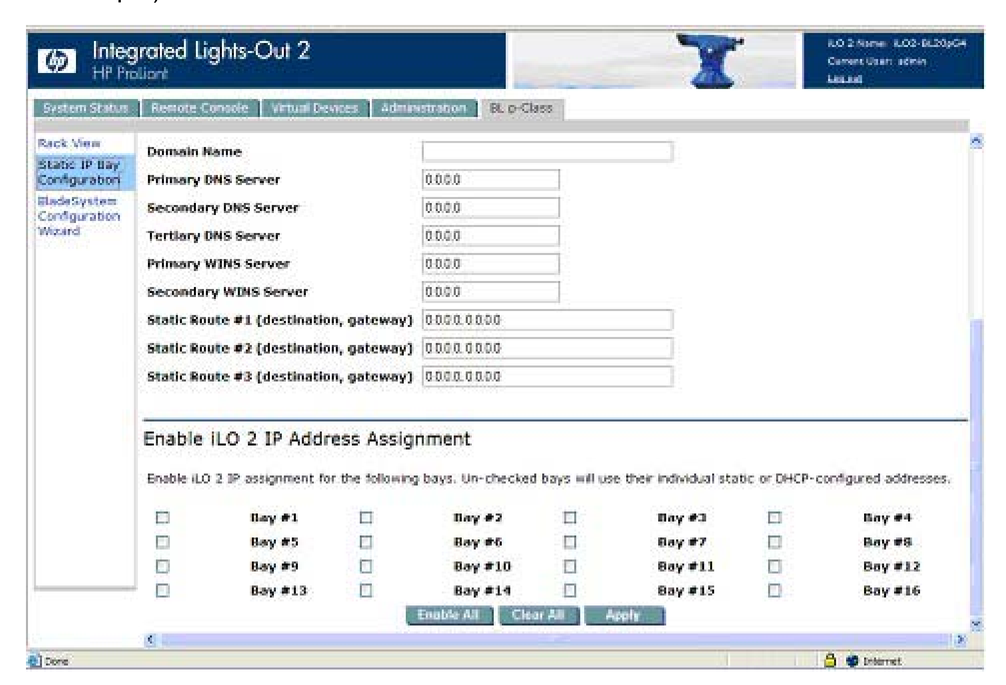
IP statique) en marquant le masque d'activation du compartiment n° 1. Avant de réinitialiser la lame, naviguez vers la page Network Settings (Paramètres réseau), sélectionnez **Enable Static IP Settings** (Activer les paramètres de configuration IP statique), puis cliquez sur **Apply** (Appliquer) pour forcer la réinitialisation de la lame et utiliser la nouvelle adresse IP statique de boîtier affectée.

Si vous déployez plusieurs boîtiers en même temps, vous pouvez facilement répéter ce processus en déplaçant un serveur lame unique dans le compartiment n°1 de chaque boîtier afin d'effectuer la configuration.

Définition des paramètres de configuration IP statique

Les paramètres de configuration IP statique disponibles dans l'onglet BL p-Class permettent de configurer et de déployer le serveur lame. Lors de la configuration de ces paramètres, vous devez utiliser la lame du compartiment 1.

La case à cocher Enable Static IP Bay Configuration Settings (Activer les paramètres de configuration IP statique), disponible dans l'onglet Network Settings (Paramètres réseau) (non représenté), permet d'activer ou de désactiver Static IP Bay Configuration (Configuration IP statique). La nouvelle option Enable Static IP Bay Configuration Settings (Activer les paramètres de configuration IP statique) est uniquement disponible sur les serveurs lame. Lorsque cette option est activée, tous les champs, à l'exception de iLO 2 Subsystem Name (Nom du sous-système iLO 2), sont désactivés. Les options Static IP Bay Configuration (Configuration IP statique) et DHCP ne peuvent pas être activées en même temps. Leur désactivation indique à iLO 2 qu'il faut utiliser une adresse IP définie par l'utilisateur. L'option Enable Static IP Bay Configuration Settings (Activer les paramètres de configuration IP statique) reste désactivée si l'infrastructure ne prend pas en charge l'option Static IP Bay Configuration (Configuration IP statique).



Paramètres de configuration standard des serveurs ProLiant BL p-Class

Beginning IP Address (Bay 1) (Adresse IP de début - Compartiment 1) : affecte l'adresse IP de début. Toutes les adresses IP doivent être valides.

Ending IP Address (Bay 16) (Adresse IP de fin - Compartiment 16) : affecte l'adresse IP de fin. Toutes les adresses IP doivent être valides.

Subnet Mask (Masque de sous-réseau) : affecte le masque de sous-réseau correspondant à la passerelle par défaut. Ce champ peut être renseigné si l'option Static IP Bay Configuration (Configuration IP statique) ou DHCP est activée. La plage d'adresses IP doit être conforme au masque de sous-réseau.

Gateway IP Address (Adresse IP de la passerelle) : affecte l'adresse IP du routeur de réseau qui relie le sous-réseau Remote Insight à un autre sous-réseau où réside la station de supervision. Ce champ peut être renseigné si l'option Static IP Bay Configuration (Configuration IP statique) ou DHCP est activée.

Paramètres de configuration avancés des serveurs ProLiant BL p-Class

Domain Name (Nom de domaine) : permet d'affecter le nom du domaine auquel iLO 2 appartiendra.

Primary DNS Server (Serveur DNS principal) : affecte une adresse IP unique de serveur DNS sur le réseau.

Secondary DNS Server (Serveur DNS secondaire) : affecte une adresse IP unique de serveur DNS sur le réseau.

Tertiary DNS Server (Serveur DNS tertiaire) : affecte une adresse IP unique de serveur DNS sur le réseau.

Primary WINS Server (Serveur WINS principal) : affecte une adresse IP unique de serveur WINS sur le réseau.

Secondary WINS Server (Serveur WINS secondaire) : affecte une adresse IP unique de serveur WINS sur le réseau.

Static Route #1, #2, and #3 (destination, gateway) (Route statique n° 1, n° 2 et n° 3 - destination, passerelle) : affecte les adresses IP de passerelle et de destination pour la route statique sur le réseau (les valeurs IP par défaut sont 0.0.0.0 et 0.0.0.0, où la première adresse IP correspond à celle de la destination, et la deuxième à celle de la passerelle).

Activation de l'affectation de l'adresse IP iLO 2

Les cases à cocher bay #1 (compartiment n°1) à bay #16 (compartiment n°16) permettent de sélectionner les serveurs lame BL p-Class à configurer. Vous pouvez sélectionner Enable All (Activer tout), Clear All (Effacer tout) ou Apply (Appliquer).

Installation HP BladeSystem

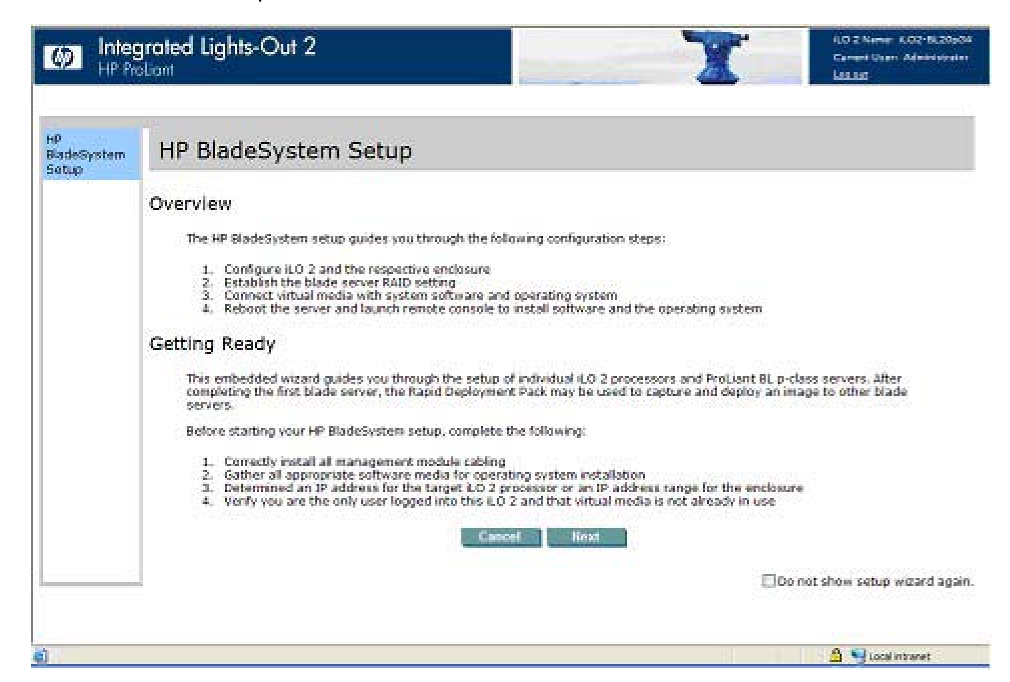
L'assistant d'installation HP BladeSystem fournit des instructions détaillées qui facilitent l'installation d'un serveur lame unique sans utiliser les protocoles DHCP ni PXE. La page d'installation HP BladeSystem s'affiche après authentification sur iLO 2 à partir du port frontal.

La lame de serveur doit être correctement connectée pour assurer la connectivité iLO 2. Connectez le serveur lame via le port E/S du serveur lame, pendant que le serveur lame est dans le rack. Cette méthode nécessite la connexion du câble d'E/S local au port d'E/S et à un PC client. À l'aide de l'adresse IP fixe inscrite sur l'étiquette du câble d'E/S et des informations de l'accès initial figurant à l'avant du serveur lame, vous pouvez accéder au serveur lame via la carte iLO 2 et l'interface de son navigateur Web standard.

L'accès s'effectue via n'importe quelle lame. En revanche, lorsque la configuration IP statique est utilisée pour définir les paramètres réseau iLO 2, l'accès se fait par le premier serveur lame du boîtier.

La première page de l'assistant se lance automatiquement si :

- le serveur est neuf et que vous vous êtes connecté à la carte iLO 2 à partir du port frontal ;
- vous n'avez pas fermé l'assistant en sélectionnant **Finish** (Terminer) sur la dernière page et si vous n'avez pas choisi l'option **Do not show setup wizard again** (Ne plus afficher l'assistant d'installation) et cliqué sur **Cancel** (Annuler) sur la première page ;
- les valeurs d'usine par défaut ont été rétablies sur iLO 2.



Cliquez sur **Cancel** (Annuler) pour fermer l'assistant d'installation automatique. Cliquez sur **Next** (Suivant) pour configurer votre serveur lame. Suivez les instruction de l'assistant d'installation pour :

1. la configuration de iLO 2
2. la vérification serveur RAID
3. la connexion à l'écran Virtual Media (support virtuel)
4. l'installation logicielle

Ecran configuration iLO 2

Cet écran permet de modifier les paramètres suivants :

- Mot de passe administrateur. HP vous conseille de remplacer le mot de passe par défaut.
- Paramètres de configuration du réseau. Les paramètres par défaut sont les suivants :
  - Enable DHCP (Activer DHCP) : Yes (oui)
  - Enable Static IP Bay Configuration (Activer la configuration IP statique) : No (non)
- Activation de Static IP Bay configuration (Configuration IP statique) afin de préconfigurer l'adresse statique des autres processeurs iLO 2 dans le boîtier, lors d'une connexion au serveur lame dans le connecteur du boîtier 1.

Par défaut, la carte iLO 2 mise à jour obtient son adresse IP via le protocole DHCP. Les autres processeurs iLO 2 du boîtier doivent être configurés séparément. Si ces paramètres ne sont pas

modifiés, cliquez sur **Next** (Suivant) pour afficher la page suivante de l'assistant d'installation. Lorsque l'un de ces paramètres est modifié, iLO 2 redémarre pour valider les paramètres mis à jour.

Les combinaisons de configuration suivantes sont également disponibles (le paramètre par défaut est entre parenthèses) :

- Enable DHCP (Yes) [Activer DHCP (Oui)] et Enable Static IP Bay Configuration (Yes) [Activer la configuration IP statique (Oui)]

  Cette configuration permet à la carte iLO 2 configurée d'obtenir son adresse IP via DHCP. Depuis la page Static IP Bay Configuration (Configuration IP statique), qui s'affiche lorsque vous cliquez sur **Next** (Suivant), vous pouvez indiquer les adresses IP des autres cartes iLO 2 du boîtier. Après avoir cliqué sur **Next** (Suivant), vous êtes invité à confirmer que vous souhaitez utiliser le protocole DHCP pour l'adresse IP de cette carte iLO 2.

- Enable DHCP (No) [Activer DHCP (Non)] et Enable Static IP Bay Configuration (Yes) [Activer la configuration IP statique (Oui)]

  Cette configuration permet à la carte iLO 2 configurée de définir son adresse IP selon les paramètres indiqués à la page Static IP Bay Configuration (Configuration IP statique). Cliquez sur **Next** (Suivant) pour afficher la page Static IP Bay Configuration (Configuration IP statique).

- Enable DHCP (No) [Activer DHCP (Non)] et Enable Static IP Bay Configuration (No) [Activer la configuration IP statique (Non)]

  Grâce à cette configuration, la carte iLO 2 configurée peut définir son adresse IP selon les paramètres indiqués à la page Network Settings (Paramètres réseau). Cliquez sur **Next** (Suivant) pour afficher la page Network Settings (Paramètres réseau).

Pour enregistrer des modifications apportées au réseau, vous devez disposer du privilège Configure iLO 2 (Configurer iLO 2).

Cliquez sur **Next** (Suivant) pour enregistrer les modifications et continuer.

Vérification de l'écran de configuration du serveur RAID

Cette étape de l'assistant d'installation permet de vérifier et d'accepter les paramètres de configuration du serveur RAID. Vérifiez le niveau RAID détecté pour les disques durs du serveur lame affiché sur la page Web et effectuez l'une des opérations suivantes :

- Cliquez sur **Next** (Suivant) pour conserver les paramètres RAID existants.
- Cliquez sur **Default Settings** (Paramètres par défaut) pour configurer automatiquement le niveau RAID en fonction du nombre de lecteurs installés. Le système vous demande de confirmer la réinitialisation du niveau RAID car cette opération risque d'entraîner une perte de données. Une mise sous tension ou un redémarrage du serveur est nécessaire pour réinitialiser le niveau RAID. Une page signalant cette opération apparaît. La page est actualisée automatiquement toutes les 10 secondes. Après le redémarrage du serveur, la page suivante de l'assistant d'installation s'affiche à nouveau. Si une erreur est détectée pendant l'opération de réinitialisation du niveau RAID, la page de configuration réapparaît et indique l'erreur rencontrée. Il y a plus de chances qu'une erreur se produise pendant l'auto-test de mise sous tension (POST) du serveur. Si c'est le cas, quittez tous les programmes RBSU ouverts, attendez la fin de l'auto-test puis relancez l'opération.

Vous pouvez modifier le niveau RAID manuellement à l'aide de RBSU. Si le système d'exploitation est déjà installé, la modification du niveau RAID risque d'entraîner une perte de données.

Connexion à l'écran Virtual Media (Support virtuel)

Cette étape de l'assistant d'installation permet de vérifier et d'accepter le lecteur que vous allez utiliser au cours de l'installation du système d'exploitation. Sous Settings (paramètres), sélectionnez le lecteur local et le type de support que vous souhaitez utiliser pendant l'installation du système d'exploitation. Cliquez sur **Launch Virtual Media** (Lancer le support virtuel) pour lancer l'applet Virtual Media.

- Assurez-vous que le support du système d'exploitation est connecté. Dans l'applet Virtual Media, une icône verte apparaît en regard du support sélectionné.
- Vérifiez que le support du système d'exploitation est dans le lecteur approprié.
- Acceptez les certificats de sécurité, dès qu'ils s'affichent.

Une fois la sélection terminée, cliquez sur **Next** (Suivant) pour enregistrer vos paramètres et continuer. L'applet Virtual Media (Support virtuel) apparaît. Lorsque l'applet est disponible, vous pouvez changer le lecteur sélectionné ou sélectionner d'autres options non répertoriées dans la page de l'assistant d'installation.

Écran d'installation logicielle

Cette étape de l'assistant d'installation permet de lancer la console distante et d'installer le système d'exploitation. Pour démarrer le processus d'installation du système d'exploitation :

- Cliquez sur **Launch Software Installation** (Lancer l'installation du logiciel) pour lancer la console distante. Automatiquement, iLO 2 met sous tension ou redémarre le serveur pour lancer l'installation du système d'exploitation via le support virtuel sélectionné précédemment.
- Acceptez les certificats de sécurité, dès qu'ils s'affichent.

Cliquez sur **Finish** (Terminer) pour terminer le processus d'installation.

Paramètres de configuration du port de diagnostic iLO 2

Le port de diagnostic iLO 2 à l'avant des serveurs ProLiant BL p-Class permet de consulter et de résoudre les problèmes du serveur à l'aide du câble de diagnostic. Le port de diagnostic iLO 2 utilise une adresse IP statique. Il n'utilise pas DHCP pour obtenir une adresse IP, pour s'enregistrer auprès de WINS ou du service DNS dynamique, ou pour utiliser une passerelle. Le câble du port de diagnostic ne doit pas rester branché lorsque la connexion réseau n'est pas active car cela pourrait affecter les performances du réseau sur le port réseau iLO 2 standard.

Les options Network Settings (Paramètres réseau) permettent de configurer les informations spécifiques au port de diagnostic. Pour plus d'informations sur l'utilisation du port et du câble de diagnostic, reportez-vous au manuel d'installation et de configuration de votre serveur lame.

Les champs suivants peuvent être configurés pour le port de diagnostic :

- Enable NIC (Activer la carte réseau)

  Si cette option est paramétrée sur Yes (Oui), le port de diagnostic est activé.
- Transceiver Speed Autoselect (Sélection automatique de la vitesse du transceiver)
- Vitesse
- Duplex
- IP Address (Adresse IP)

Utilisez ce paramètre pour attribuer une adresse IP statique à iLO 2 sur votre réseau. Par défaut, l'adresse IP est attribuée par DHCP. Par défaut, l'adresse IP est 192.168.1.1 pour tous les ports de diagnostic iLO 2.

- Subnet Mask (Masque de sous-réseau)
  - Utilisez ce paramètre pour attribuer le masque de sous-réseau du port de diagnostic iLO 2. Par défaut, le masque de sous-réseau est 255.255.255.0 pour tous les ports de diagnostic iLO 2.
  - L'utilisation du port de diagnostic est automatiquement détectée lorsqu'un câble réseau actif y est raccordé. Lors du basculement entre le port de diagnostic et le port arrière, vous devez attendre que la commutation réseau soit terminée (environ 90 secondes) avant de tenter de vous connecter à l'aide du navigateur.

  REMARQUE : le port de diagnostic n'est pas commuté si une session de console distante est active ou qu'une mise à jour du microprogramme est en cours.

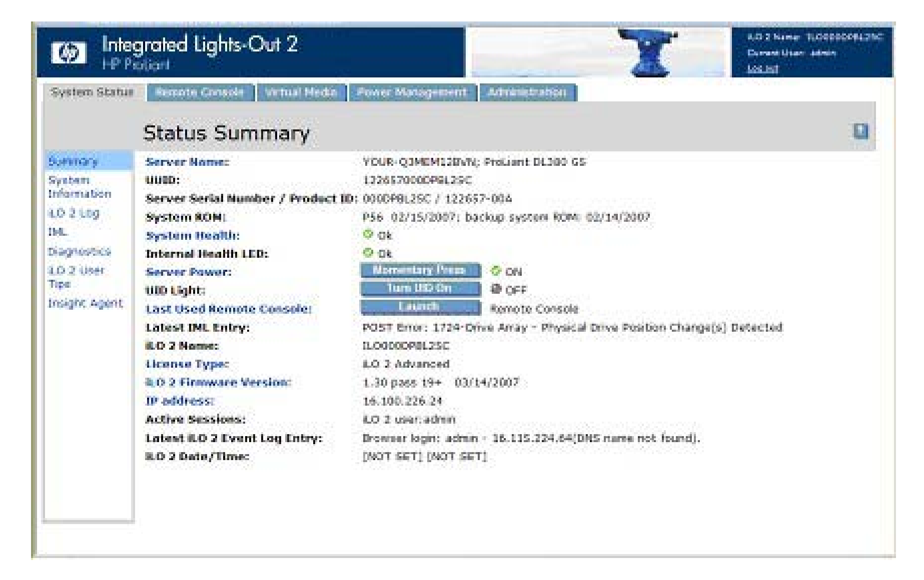
4 Utilisation de iLO 2

Cette section traite des rubriques suivantes :

État du système et informations sur l'état du système

Lorsque vous accédez à iLO 2 pour la première fois, l'interface affiche la page Status Summary (Récapitulatif de l'état) contenant des informations sur l'état du système et le récapitulatif de l'état, et permet d'accéder aux informations d'état, aux journaux système et aux informations Insight Agent. La section System Status (État du système) contient les options suivantes : Summary (Résumé), System Information (Informations système), iLO 2 Log (Journal iLO 2), IML, Diagnostics, iLO 2 User Tips (Conseils utilisateur iLO 2) et Insight Agents (Agents Insight).

La page Status Summary (Récapitulatif de l'état) affiche des détails de niveau supérieur concernant le système et le sous-système iLO 2, ainsi que des liens vers des fonctions courantes. Pour accéder à la page Status Summary (Récapitulatif de l'état) depuis d'autres parties de l'interface iLO 2, cliquez sur **System Status>Summary** (État du système>Résumé).



Les informations sur l'état sont les suivantes :

- Server Name (Nom du serveur) : affiche le nom du serveur. Lorsque vous cliquez sur cet intitulé d'option, vous accédez à la page Administration>Options>Access (Administration>Options>Accès).
- UUID : affiche l'ID du serveur.
- Server Serial Number/Product ID (Numéro de série/ID produit du serveur) : affiche le numéro de série du serveur qui est affecté lors de la fabrication du système. Vous pouvez modifier ce paramètre à l'aide de l'utilitaire RBSU du système pendant le POST. L'ID du produit permet d'effectuer la distinction entre différents systèmes associés à un même numéro de série. L'ID produit est attribué lors de la fabrication du système, ce qui ne vous empêche pas pour autant de le modifier à l'aide de l'utilitaire RBSU du système pendant le POST.
- System ROM (ROM système) : affiche la famille et la version de la ROM système active. Si le système prend en charge une ROM système de sauvegarde, une date de sauvegarde est également affichée.
- System Health (État du système) : présente un résumé de l'état des sous-systèmes surveillés, notamment l'état global et la redondance (capacité à gérer une panne). Lorsque vous cliquez sur cet intitulé d'option, vous accédez à la page System>Status>System Information Summary (Système>État>Résumé des informations système).
- Internal Health LED (Voyant état interne) : représente l'indicateur de l'état interne du serveur (en cas de prise en charge). Les problèmes de ventilateurs, de capteurs de température, de tensions et d'autres sous-systèmes contrôlés sur le serveur sont également résumés. Pour plus d'informations, reportez-vous à la section « Résumé des informations système » (Résumé des informations système à la page 83).
- TPM Status (État TPM) : affiche la configuration d'état TPM. Lorsque le module TPM n'est pas pris en charge sur le système hôte ou la ROM système, son état n'est pas indiqué sur la page Status Summary (Récapitulatif de l'état). Pour plus d'informations, reportez-vous à la section « Prise en charge du module TPM (Trusted Platform Module) ».
- Server Power (Alimentation du serveur) : affiche l'état de l'alimentation du serveur (ON/STANDBY) au moment du chargement de la page. Lorsque vous cliquez sur cet intitulé d'option, vous accédez à la page Server>Power Management (Serveur>Gestion de l'alimentation). Les utilisateurs disposant du privilège Virtual Power and Reset (Alimentation et réinitialisation virtuelles) peuvent également utiliser le bouton Momentary Press (Pression brève).
- UID Light (Voyant UID) : affiche l'état du voyant UID au moment du chargement de la page. Vous pouvez contrôler cet état à l'aide du bouton Turn UID On (Allumer le voyant UID) et des boutons situés sur le châssis du serveur.

  L'UID vous aide à identifier et à localiser un système, particulièrement dans des environnements contenant un grand nombre de racks. De plus, l'UID sert à indiquer qu'une opération critique est en cours sur l'hôte, telle qu'un accès à la console distante ou une mise à jour du microprogramme.

  △ **ATTENTION :** Ne mettez jamais un serveur hors tension lorsque le voyant UID clignote.

  L'état en cours de l'UID (marche ou arrêt) correspond au dernier état choisi à l'aide d'une de ces méthodes. Lorsqu'un nouvel état est choisi pendant que l'UID clignote, celui-ci devient l'état en cours et prend effet dès l'arrêt du clignotement de l'UID. Lorsque l'UID clignote, l'état de l'UID en cours s'affiche et l'étiquette se met à clignoter. Lorsque que l'UID cesse de clignoter, l'étiquette est supprimée.

  L'UID n'est pas pris en charge par HP ProLiant ML310 G3.

- Last Used Remote Console (Dernière console distante utilisée) : affiche la console distante qui a été lancée précédemment, ainsi que sa disponibilité. Ceci vous permet de lancer rapidement votre console distante favorite. La console distante ne peut être utilisée que si elle est disponible et si vous disposez des privilèges utilisateur appropriés. Vous pouvez choisir une autre console en suivant le lien Last Used Remote Console (Dernière console distante utilisée).
- Latest IML Entry (Dernière entrée IML) : affiche l'entrée la plus récente dans l'IML.
- iLO 2 Name (Nom iLO 2) : affiche le nom affecté au sous-système iLO 2. Par défaut, il s'agit du mot iLO ajouté au numéro de série du système. Cette valeur est utilisée pour le nom du réseau et doit être unique.
- License Type (Type de licence) : indique si une licence est installée sur le système. Lorsque vous cliquez sur cet intitulé d'option, vous accédez à la page Administration>Licensing (Administration>Licence). Certaines fonctions de iLO 2 ne peuvent être utilisées qu'avec une licence.
- iLO 2 Firmware Version (Version du microprogramme iLO 2) : affiche des informations sur la version du microprogramme iLO 2 installé. Lorsque vous cliquez sur cet intitulé d'option, vous accédez à la page iLO 2 Release Notes (Notes de mise à jour iLO 2) qui souligne les nouvelles fonctionnalités présentes dans la version du microprogramme en cours et dans les versions précédentes sélectionnées.
- IP Address (Adresse IP) : affiche l'adresse IP réseau du sous-système iLO 2. Lorsque vous cliquez sur cet intitulé d'option, vous accédez à la page Administration>Network Settings (Administration>Paramètres réseau).
- Active Sessions (Sessions actives) : liste l'ensemble des utilisateurs actuellement connectés à iLO 2.
- Latest iLO 2 Event Log Entry (Dernière entrée du journal des événements iLO 2) : affiche l'entrée la plus récente du journal des événements iLO 2.
- iLO 2 Date (Date iLO 2) : affiche la date (MM/JJ/AAAA) comme indiqué par le calendrier interne du sous-système iLO 2. Le calendrier interne iLO 2 est synchronisé avec le système hôte lors du test POST et lorsque les agents Insight sont exécutés.
- iLO 2 Date/Time (Date/heure iLO 2) : affiche l'horloge interne du sous-système iLO 2. L'horloge interne iLO 2 est synchronisée avec le système hôte lors du test POST et lorsque les agents Insight sont exécutés.

Résumé des informations système

L'option System Information (Informations système) affiche l'état du système surveillé. De nombreuses fonctionnalités indispensables au fonctionnement et à la gestion des composants du serveur HP ProLiant ont migré du driver d'état au microprocesseur de iLO 2. Ces fonctionnalités sont disponibles sans installation ni chargement du driver d'état du système d'exploitation installé. Le microprocesseur iLO 2 surveille ces périphériques lors de la mise sous tension du serveur au cours de son réamorçage, l'initialisation du système d'exploitation et du fonctionnement. La surveillance continue en cas de panne inopinée du système d'exploitation. Pour accéder aux informations système, cliquez sur **System Status>System Information** (État du système>Informations système). L'onglet System Health Summary (Résumé sur l'état du système) s'affiche. Les informations système affichent également les onglets intégrés relatifs à l'état suivants : Fans - Ventilateurs (Ventilateurs à la page 84), Temperatures - Températures (Températures à la page 85), Power - Alimentation (Alimentation à la page 85), Processors - Processeurs (Processeurs à la page 86), Memory - Mémoire (Mémoire à la page 86) et NIC - Cartes réseau (NIC à la page 86).

L'onglet Summary (Résumé) affiche l'état des sous-systèmes de plate-forme hôtes en un clin d'oeil, récapitulant la condition des sous-systèmes surveillés, notamment l'état global et la redondance

(capacité à gérer une panne). Les sous-systèmes peuvent comprendre des ventilateurs, des capteurs de température, des blocs d'alimentation et des modules régulateurs de tension.

- Fans (Ventilateurs) : affiche l'état des ventilateurs remplaçables dans le châssis du serveur. Ces données indiquent la zone refroidie par chaque ventilateur et les vitesses actuelles des ventilateurs.
- Temperatures (Températures) : affiche les conditions de température surveillées au niveau des capteurs installés à divers emplacements dans le châssis du serveur, et la température du processeur. La surveillance de la température permet de conserver la température à un niveau inférieur au seuil de précaution. Si la température dépasse le seuil de précaution, la vitesse des ventilateurs est amenée à son maximum.
- VRMs (VRM) : affiche l'état des modules VRM. Un module VRM est requis pour chaque processeur du système. Le module VRM régule l'alimentation pour qu'elle soit en phase avec les caractéristiques d'alimentation du processeur pris en charge. Un module VRM en panne empêche la prise en charge du processeur et doit être remplacé.
- Power Supplies (Blocs d'alimentation) : affiche la présence et la condition des blocs d'alimentation installés.
  - OK : indique que l'alimentation est installée et opérationnelle.
  - Unpowered (Hors tension) : indique que le bloc d'alimentation est installé, mais pas opérationnel. Vérifiez que le cordon d'alimentation est branché.
  - Not present (Absent) : indique que le bloc d'alimentation n'est pas installé. L'alimentation n'est pas redondante dans cette condition.
  - Failed (En panne) : indique que le bloc d'alimentation doit être remplacé.

Pour accéder à l'onglet Summary (Résumé) depuis d'autres parties de l'interface iLO 2, cliquez sur **System Status>System Information>Summary** (État du système>Informations système>Résumé).

Ventilateurs

À l'aide d'un équipement matériel supplémentaire, iLO 2 contrôle le fonctionnement et la vitesse des ventilateurs. Les ventilateurs apportent le refroidissement indispensable des composants pour garantir la fiabilité et le fonctionnement normal. L'emplacement, la position, la conception et le contrôle de la vitesse des ventilateurs prennent en compte les différentes températures surveillées dans tout le système pour fournir le refroidissement approprié avec de faibles niveaux sonores.

Les règles de fonctionnement des ventilateurs peuvent varier d'un serveur à l'autre en fonction de la configuration des ventilateurs et du niveau de refroidissement requis. Le contrôle des ventilateurs tient compte de la température interne du système, en augmentant ou en réduisant la vitesse selon le niveau de refroidissement requis. Dans le cas improbable d'une panne de ventilateur, certaines stratégies de fonctionnement des ventilateurs peuvent augmenter la vitesse des autres ventilateurs, enregistrer l'événement dans l'IML et allumer des voyants.

La surveillance du sous-système des ventilateurs comprend les configurations suffisantes, redondantes et non redondantes des ventilateurs. Une panne de ventilateur se produit rarement, mais pour garantir la fiabilité et un fonctionnement normal, les serveurs ProLiant disposent de configurations redondantes de ventilateurs. Dans les serveurs ProLiant prenant en charge les configurations redondantes, le ou les ventilateurs peuvent tomber en panne et continuer cependant à fournir un refroidissement suffisant pour assurer un bon fonctionnement. iLO 2 renforce le contrôle des ventilateurs afin de maintenir le fonctionnement du serveur en toute sécurité en cas de panne d'un ventilateur, d'opération de maintenance ou de tout autre événement modifiant le refroidissement du serveur.

Dans les configurations non redondantes, ou dans les configurations redondantes où plusieurs ventilateurs tombent en panne, le système peut ne plus être en mesure de fournir le refroidissement

nécessaire pour empêcher sa détérioration et garantir l'intégrité des données. Dans ce cas, outre les stratégies de refroidissement, le système peut exécuter un arrêt sans perte de données du système d'exploitation et du serveur.

L'onglet Fan (Ventilateur) affiche l'état des ventilateurs remplaçables dans le châssis du serveur. Ces données indiquent la zone refroidie par chaque ventilateur et la vitesse actuelle des ventilateurs.

Températures

L'onglet Temperatures (Températures) affiche l'emplacement, l'état, la température et les paramètres de seuil pour les capteurs de température du châssis du serveur. La surveillance de la température permet de conserver la température à un niveau inférieur au seuil de précaution. Si un ou plusieurs capteurs dépassent ce seuil, iLO 2 applique la stratégie de récupération, afin d'empêcher la détérioration des composants du serveur.

- Si la température dépasse le seuil de précaution, la vitesse des ventilateurs est amenée à son maximum.
- Si la température dépasse le seuil critique, le système tente un arrêt du serveur sans perte de données.
- Si la température dépasse le seuil fatal, le serveur s'éteint immédiatement pour empêcher une panne définitive.

Les stratégies de surveillance varient en fonction des conditions requises pour le serveur. Les stratégies comprennent généralement l'augmentation de la vitesse des ventilateurs à un niveau de refroidissement maximum, la consignation de l'événement concernant la température dans le journal IML, l'affichage d'un indicateur visuel de l'événement à l'aide de voyants et l'arrêt sans perte de données du système d'exploitation.

Une fois les problèmes de température excessive résolus, d'autres stratégies sont mises en œuvre, notamment le retour de la vitesse des ventilateurs à la normale, l'enregistrement de l'événement dans l'IML, la désactivation des voyants et, le cas échéant, l'annulation des arrêts en cours.

Alimentation

L'onglet VRMs/Power Supplies (VRM/Blocs d'alimentation) affiche l'état de chaque VRM ou bloc d'alimentation. Les modules VRM sont requis pour chaque processeur du système. Ils régulent l'alimentation pour qu'elle soit en phase avec les besoins du processeur pris en charge. Il est possible de remplacer un module VRM en panne. La panne d'un module VRM empêche la prise en charge du processeur.

iLO 2 surveille également les blocs d'alimentation du système pour optimiser le temps de fonctionnement du serveur et du système d'exploitation. Les blocs d'alimentation peuvent être affectés par des baisses de tension et d'autres problèmes d'alimentation, ou encore par un débranchement accidentel des cordons d'alimentation secteur. Ces problèmes provoquent une perte de redondance si des blocs d'alimentation redondants sont en place, ou encore un arrêt si ces blocs ne sont pas utilisés. Par ailleurs, en cas de panne d'un bloc d'alimentation (panne matérielle) ou de débranchement du cordon d'alimentation secteur, les événements appropriés sont enregistrés dans l'IML et les voyants s'allument.

iLO 2 surveille les blocs d'alimentation pour vérifier qu'ils sont correctement installés. Ces informations s'affichent sur la page System Information (Informations système). La page Reviewing the System Information (Vérification des informations système) et l'IML vous aident à choisir à quel moment réparer ou remplacer un bloc d'alimentation, afin d'empêcher l'interruption d'un service.

Processeurs

L'onglet Processors (Processeurs) affiche les connecteurs de processeurs disponibles, le type de processeur installé dans le connecteur et un bref récapitulatif de l'état du sous-système du processeur. La vitesse en MHz du processeur installé et les fonctionnalités relatives au cache s'affichent, le cas échéant.

Mémoire

L'onglet Memory (Mémoire) affiche les emplacements de mémoire disponibles et le type de mémoire installé à cet emplacement, le cas échéant.

NIC

L'onglet NIC (Cartes réseau) affiche les adresses MAC des cartes réseau intégrées. Cette page n'affiche pas les adaptateurs réseau.

Journal iLO 2

La page iLO 2 Log (Journal iLO 2) affiche le journal d'événements iLO 2. Il contient l'enregistrement des événements significatifs détectés par iLO 2. Les événements de ce journal comprennent les événements majeurs du serveur, tels qu'une panne de courant du serveur ou une réinitialisation du serveur, ainsi que les événements iLO 2, tels que des tentatives de connexion non autorisées. Les autres événements de ce journal concernent toutes les connexions, ayant échoué ou non, au navigateur et à la console distante, l'alimentation virtuelle et la mise sous tension, les actions de suppression du journal d'événements et certaines modifications de configuration, telles que la création ou la suppression d'un utilisateur.

La carte iLO 2 assure le codage sécurisé des mots de passe, effectue le suivi de toutes les tentatives d'ouverture de session et conserve un enregistrement de tous les échecs d'ouverture de session. La fonction Authentication Failure Logging (Consignation des échecs d'authentification) permet de configurer des critères de consignation pour les authentifications qui ont échoué. Vous pouvez configurer le suivi des échec de tentatives de connexion pour chaque tentative ou pour une tentative sur deux, trois ou cinq, et enregistrer le nom du client pour chaque entrée consignée afin d'améliorer les fonctionnalités d'audit dans des environnements DHCP. Vous pouvez également configurer l'enregistrement du nom de compte, du nom de l'ordinateur et de l'adresse IP. Lorsque la tentative de connexion échoue, iLO 2 génère également des alertes et les envoie à une console de supervision distante.

Les événements enregistrés par des versions ultérieures du microprogramme iLO 2 peuvent ne pas être pris en charge par des versions antérieures. Lorsqu'un événement est enregistré par un microprogramme non pris en charge, il est répertorié en tant que `UNKNOWN EVENT TYPE` (Type d'événement inconnu). Vous pouvez effacer le journal des événements pour supprimer ces entrées ou mettre à niveau le microprogramme vers la dernière version prise en charge.

Pour accéder au journal iLO 2, cliquez sur **System Status>iLO 2 Log** (État du système>Journal iLO 2).

Pour effacer le journal des événements :

1. Cliquez sur **Clear Event Log** (Effacer journal des événements) pour effacer toutes les informations consignées dans le journal des événements.
2. Cliquez sur **OK** pour confirmer la suppression des enregistrements du journal. Une ligne indiquant que le journal a été effacé est consignée dans le journal.

IML

La page IML affiche le journal Integrate Management Log (Journal de maintenance intégré). Ce journal est un enregistrement des événements historiques ayant eu lieu sur le serveur et rapportés par divers composants logiciel. Les événements sont générés par la ROM système et par des services tels que le driver de supervision du système (état). Le journal de maintenance intégré (IML) permet d'afficher les événements consignés relatifs au serveur distant. Les événements enregistrés incluent tous les événements propres au serveur enregistrés par le driver d'état du système, y compris les informations du système d'exploitation et les codes POST basés sur la ROM. Pour plus d'informations, reportez-vous au manuel de votre serveur.

Les entrées de l'IML peuvent aider lors du diagnostic des problèmes ou lors d'actions de prévention. Des actions de prévention sont recommandées afin d'éviter tout dysfonctionnement du service. iLO 2 gère l'IML accessible via un navigateur pris en charge, même lorsque le service est arrêté. Cette particularité peut être utile lors du dépannage de problèmes sur le serveur hôte distant.

Pour trier les événements du journal, cliquez sur l'en-tête des colonnes de données. Une fois le tri terminé, cliquer à nouveau sur l'en-tête inverse l'ordre en cours de la colonne. Si les journaux sont très volumineux, le tri et l'affichage peuvent prendre plusieurs minutes. Vous pouvez effacer les événements de ce journal à partir de la page d'accueil du serveur des agents Web Insight Manager.

Le processeur iLO 2 enregistre les informations suivantes sur l'IML en fonctions des occurrences du système.

- Ventilateur inséré
- Ventilateur supprimé
- Panne du ventilateur
- Ventilateur endommagé
- Ventilateur réparé
- Perte de redondance du ventilateur
- Ventilateurs redondants
- Bloc d'alimentation inséré
- Bloc d'alimentation supprimé
- Défaillance de l'alimentation
- Perte de redondance des blocs d'alimentation
- Blocs d'alimentation redondants
- Seuil de température dépassé
- Température normale
- Arrêt automatique lancé
- Arrêt automatique annulé

Diagnostics

L'option Diagnostics de l'onglet System Status (État du système) affiche l'écran Server and iLO 2 Diagnostics (Diagnostics serveur et ILO 2). Cet écran affiche les résultats de l'auto-test iLO 2 et fournit des options permettant de générer une NMI sur le système et de réinitialiser iLO 2.

REMARQUE : lorsque vous vous connectez via Diagnostics Port (Port de diagnostics), le serveur d'annuaire n'est pas disponible. Vous pouvez uniquement ouvrir une session à l'aide d'un compte local.

La page Diagnostics contient les sections suivantes :

- Bouton NMI (Non-Maskable Interrupt)

  Cette section contient le bouton Generate NMI to System (Générer NMI sur le système) qui permet d'interrompre le système d'exploitation en vue d'un débogage. Il s'agit d'une fonction avancée qui doit être exclusivement utilisée pour un débogage au niveau du noyau. Voici quelques possibilités d'utilisation de la fonction Generate NMI to System (Générer NMI sur le système) :

  - N'utilisez la fonction Demonstrate ASR (Présenter ASR) que si le driver System Management (état du système) est chargé et ASR activé. L'hôte redémarre automatiquement après une NMI (Non-Maskable Interrupt – interruption non masquable).

  - Utilisez la fonction de débogage si une application logicielle bloque le système. Le bouton Generate NMI (Générer NMI) permet d'activer le débogueur du système d'exploitation.

  - Si vous souhaitez capturer le contexte du serveur, déclenchez le vidage de la mémoire d'un hôte qui ne répond pas.

    Vous devez être doté du privilège Virtual Power and Reset (Alimentation et réinitialisation virtuelles) pour pouvoir générer une NMI. Une NMI inopinée indique généralement une condition fatale sur la plate-forme hôte. Un écran bleu, un arrêt d'urgence (panique), un ABEND (arrêt anormal) ou quelque autre exception fatale se produit lorsque le système d'exploitation hôte reçoit une NMI inopinée, même si le système d'exploitation est bloqué ou ne répond pas. La génération d'une NMI inopinée permet de diagnostiquer un système d'exploitation en état de catatonie ou d'interblocage. Cette opération entraîne le plantage du système d'exploitation, avec perte de service et de données.

    La génération d'une NMI doit être réservée aux cas diagnostiques extrêmes dans lesquels le système d'exploitation ne fonctionne plus correctement et seulement si un service d'assistance expérimenté a recommandé cette mesure. L'utilisation d'une NMI en tant qu'outil de diagnostic et de débogage est principalement utilisée lorsque le système d'exploitation n'est plus disponible. Cette mesure ne doit pas être tentée pendant le fonctionnement normal du serveur. Le bouton Generate NMI (Générer NMI) n'arrête pas le système d'exploitation de façon ordonnée.

- Résultats de l'auto-test iLO 2

  La section iLO 2 Self-Test Results (Résultats de l'auto-test iLO 2) affiche les résultats des diagnostics internes iLO 2. iLO 2 exécute une série de procédures d'initialisation et de diagnostic sur les sous-systèmes du système iLO 2. Les résultats s'affichent à l'écran Server and iLO 2 Diagnostics (Diagnostics serveur et iLO 2). Tous les sous-systèmes testés doivent indiquer Passed (Test réussi) en situation normale. Chaque test affiche l'un des trois résultats : Passed (Réussi), Fault (Échec) ou N/A (N/D).

  L'état de ces auto-tests est indiqué par les résultats des tests et a pour objet d'identifier les zones à problèmes. Si un test affiche la condition Fault (Échec), lisez attentivement toutes les informations présentées à l'écran. Les tests spécifiques qui sont exécutés sont dépendants du système. Tous les tests ne sont pas exécutés sur tous les systèmes. Reportez-vous à la page des diagnostics iLO 2 pour vérifier la liste des tests exécutés automatiquement sur votre système.

- Reset Integrated Lights-Out 2

  Cette section contient le bouton Reset (Réinitialisation) permettant de réamorcer le processeur iLO 2. La réinitialisation ne modifie pas la configuration. Elle met fin à toutes les connexions actives à iLO 2 et interrompt toutes les mises à jour de microprogramme en cours. Vous devez être doté

du privilège Configure iLO 2 (Configurer iLO 2) (configurer les paramètres d'un périphérique local) pour pouvoir réinitialiser iLO 2 à l'aide de cette option.

Agents Insight

Les agents HP Insight Management (supervision) gèrent une interface de navigateur donnant accès aux données de gestion d'exécution via la page d'accueil System Management (Gestion du système). Cette page d'accueil est une interface Web sécurisée qui renforce et simplifie la gestion de serveurs et systèmes d'exploitation individuels. Grâce au regroupement des données des agents HP Insight Management et d'autres outils, la page d'accueil System Management offre une interface intuitive permettant d'analyser en profondeur la configuration matérielle, les données d'état, les mesures de performances, les seuils système et les informations de contrôle de version du logiciel.

Les agents peuvent fournir automatiquement le lien vers iLO 2, ou vous pouvez entrer ce dernier manuellement à l'aide de Administration/Management.

Pour plus d'information, reportez-vous à la section « Intégration de HP SIM (Systems Insight Manager) » et au site Web HP (http://www.hp.com/servers/manage).

Console distante iLO 2

La fonction iLO 2 Remote Console (Console distante iLO 2) redirige la console du serveur hôte vers le navigateur du client réseau, permettant ainsi d'accéder au texte intégral (standard), à la vidéo en mode graphique, au clavier et à la souris sur le serveur hôte distant (à condition d'être sous licence). iLO 2 utilise la technologie KVM virtuelle afin que la console distante atteigne le niveau de performances des autres solutions KVM.

L'accès à la console distante permet également d'observer les messages POST d'amorçage au moment où le serveur hôte distant redémarre et lance les routines de configuration basée sur la ROM pour configurer le matériel du serveur hôte distant. Lors de l'installation de systèmes d'exploitation à distance, les consoles graphiques distantes (si sous licence) permettent d'afficher et de contrôler l'écran du serveur hôte pendant toute la procédure d'installation.

L'accès à la console distante vous donne un contrôle complet sur le serveur hôte distant comme si vous étiez devant le système, y compris l'accès au système de fichiers distant et aux unités réseau. La console distante permet de modifier les paramètres du matériel et des logiciels du serveur hôte distant, d'installer des applications et des drivers, de modifier la résolution de l'écran du serveur distant et d'arrêter le système distant de façon ordonnée.

Jusqu'à 10 utilisateurs sont autorisés à se connecter simultanément à iLO 2. Toutefois, quatre utilisateurs seulement peuvent accéder à une console distante intégrée partagée. Si vous essayez d'ouvrir la console distante alors que vous l'utilisez déjà, un message d'avertissement s'affiche indiquant qu'un autre utilisateur l'utilise. Pour plus d'informations sur la manière d'accéder à la session de console distante en cours, reportez-vous à la section « Console distante partagée » (Console distante partagée à la page 100). Pour prendre le contrôle de la session, utilisez la fonction Remote Console Acquire (Acquisition de console distante). Pour plus d'informations, reportez-vous à la section « Acquisition de la console distante » (Acquisition de la console distante à la page 104).

La page Remote Console Information (Informations sur la console distante) fournit des liens d'accès aux différentes options d'accès à la console distante. Après avoir choisi l'option à utiliser, cliquez sur le lien correspondant. iLO 2 offre les options d'accès à la console distante suivantes :

- Integrated Remote Console (Console distante intégrée) (Option Integrated Remote Console (Console distante intégrée) à la page 96) : permet d'accéder au système KVM et de contrôler les fonctions Virtual Power (Alimentation virtuelle) et Virtual Media (Support virtuel) à partir d'une seule et unique console via Microsoft® Internet Explorer.
- Integrated Remote Console Fullscreen (Mode plein écran de la console distante intégrée) (Mode plein écran de l'IRC à la page 95) : redimensionne la console distante intégrée afin qu'elle présente la même résolution d'écran que le système hôte distant.

  Les deux fonctions Integrated Remote Console (Console distante intégrée) et Integrated Remote Console Fullscreen (Mode plein écran de la console distante intégrée) utilisent ActiveX et nécessitent Microsoft® Internet Explorer™.
- Remote Console (Console distante) (Remote Console (Console distante) à la page 105) : permet d'accéder au système KVM par le biais d'une console basée sur une applet Java. La fonction Remote Console (Console distante) correspond à la version améliorée de la fonction de prise en charge de console distante familière du produit iLO d'origine. La prise en charge de la fonction Remote Console (Console distante) requiert que le système client soit équipé de Java™. Elle fonctionne avec tous les systèmes d'exploitation et navigateurs pris en charge par iLO 2.
- Remote Serial Console (Console série distante) (Remote Serial Console (Console série distante) à la page 112) : permet d'accéder à une console série VT320 à partir d'une console basée sur une applet Java connectée au Virtual Serial Port (Port série virtuel) de iLO 2. La console série distante qui est disponible sans licence supplémentaire convient aux systèmes d'exploitation hôtes n'exigeant l'accès à la console graphique.

iLO 2 Standard fournit l'accès à la console du serveur à partir du démarrage du serveur par le biais d'un test POST. Integrated Remote Console (Console distante intégrée), Integrated Remote Console Fullscreen (Plein écran de la console distante intégrée) et Remote Console (Console distante) sont des consoles distantes graphiques qui transforment un navigateur pris en charge en bureau virtuel, vous donnant ainsi un contrôle complet sur l'écran, le clavier et la souris du serveur hôte. La console, qui est indépendante du système d'exploitation, prend en charge les modes graphiques permettant d'afficher les activités du serveur hôte distant, comme les opérations d'arrêt et de démarrage (si sous licence).

L'accès de la console distante au serveur hôte après un test POST au niveau du serveur est une fonction sous licence disponible grâce à l'acquisition de licences supplémentaires. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21). Pour accéder à la fonction iLO 2 Remote Console (Console distante iLO 2), cliquez sur **Remote Console** (Console distante). La page Remote Console Information (Informations sur la console distante) s'affiche.

Présentation de la console distante et options de licence

La console distante et la console distante intégrée sont des consoles graphiques. Leur affichage s'effectue au moyen d'un programme client capable de traiter les commandes graphiques iLO 2. Deux clients sont fournis pour afficher les graphiques iLO 2 :

- Console distante basée sur Java™
- Console distante intégrée basée sur Windows® Active X

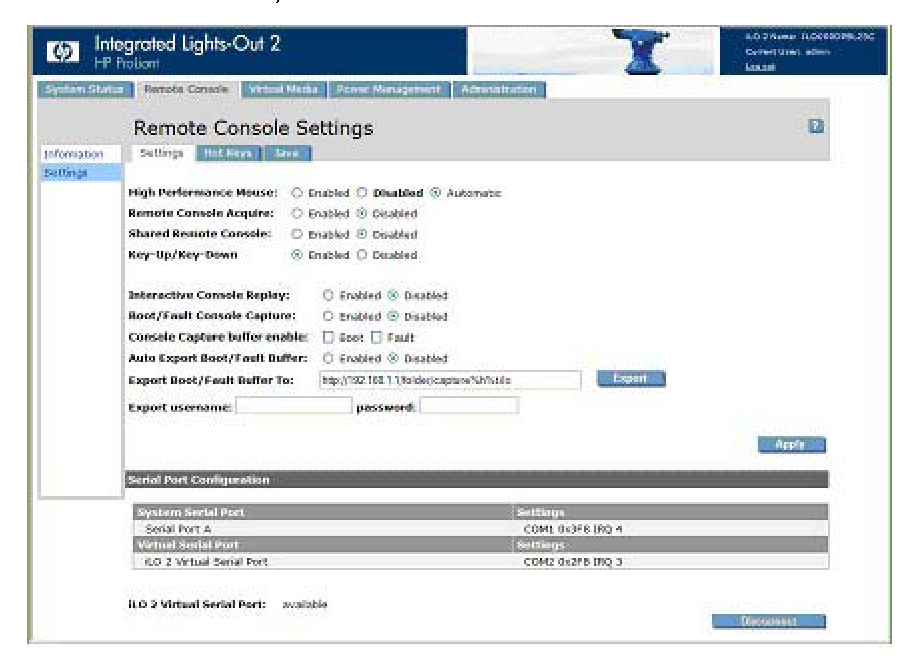
Pour les clients incapables de traiter les graphiques iLO 2 (cas de SSH et telnet), vous devez utiliser la console série distante iLO 2 ou acheter une licence iLO Advanced afin d'accéder à la console texte après la séquence POST.

Les consoles ESX, en particulier le modèle ESX 1, ne prennent pas totalement en charge la console distante et la console distante intégrée iLO 2. Par ailleurs, elles ne sont pas du tout compatibles avec la console série distante.

Les serveurs lame iLO 2 sont livrés avec iLO 2 Standard Blade Edition, qui intègre la console distante. Toutefois, les modèles HP ProLiant ML et HP ProLiant DL sont livrés avec une licence iLO Standard, qui ne comprend pas la console distante ni la console distante intégrée. Dès que le serveur commence l'amorçage d'un système d'exploitation, le module iLO 2 Standard des modèles HP ProLiant ML et ProLiant DL affiche un message demandant la licence de iLO 2. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21).

Paramètres de la console distante

Les paramètres et les options de la console distante iLO 2 sont configurés sur la page Remote Console Settings (Paramètres de la console distante). Pour accéder à la page Remote Console Settings (Paramètres de la console distante), cliquez sur **Remote Console>Settings** (Console distante>Paramètres).



La page Remote Console Settings (Paramètres de la console distante) comprend trois onglets :

Paramètres

- La fonction High Performance Mouse (Souris hautes performances) contribue à minimiser les problèmes de synchronisation de souris, mais elle n'est pas prise en charge sur tous les systèmes d'exploitation. La modification des paramètres prend effet au démarrage ou au redémarrage de la console distante. Les options suivantes sont disponibles :
  - Disabled (Désactivé) : permet à la souris d'utiliser le mode des coordonnées relatives compatible avec la plupart des systèmes d'exploitation hôtes.
  - Enabled (Activé) : permet à la souris d'utiliser le mode des coordonnées absolues, éliminant ainsi les problèmes de synchronisation sur les systèmes d'exploitation pris en charge.
  - Automatic (Automatique) : permet à iLO 2 de sélectionner le mode de la souris approprié lorsque le driver iLO 2 est chargé sur le système d'exploitation hôte. Le mode sélectionné est

permanent sauf en cas de mode différent indiqué au moment du chargement du driver du système d'exploitation ou du choix d'un autre paramètre.

- Remote Console Acquire (Acquisition de la console distante) permet à un utilisateur de prendre le contrôle de la session de console distante d'un autre utilisateur. Ce paramètre active ou désactive la fonctionnalité d'acquisition.
- Shared Remote Console (Console distante partagée) permet à plusieurs utilisateurs de visualiser et de contrôler simultanément la console du serveur. Ce paramètre active ou désactive la fonctionnalité partagée.
- Le paramètre Interactive Console Replay (Retransmission console interactive) permet de retransmettre la capture de la vidéo de la console des séquences boot et fault en même temps que les captures manuelles de la console initiées par l'utilisateur.
- Le paramètre Key-Up/Key-Down (Touche haut/Touche bas) permet de basculer entre le modèle de clavier de rapport HID et le modèle de clavier de codes ASCII et ÉCHAP dans l'IRC. Le modèle de clavier de rapport HID est activé par défaut mais peut entraîner la répétition des caractères sur des réseaux à temps d'attente élevé. Si vous rencontrez des caractères répétés lors de l'utilisation de l'IRC, définissez Key-Up/Key-Down (Touche haut/Touche bas) sur **Disabled** (Désactivé).
- Boot/Fault Console Capture (Capture console boot/fault) permet de capturer la vidéo de console des séquences boot et fault afin de la stocker dans les mémoires tampons internes. L'espace de la mémoire tampon interne est limité à la capture de la séquence boot ou fault la plus récente. L'espace de la mémoire tampon est limité. Plus la résolution graphique de la console du serveur est dynamique et élevée, moins la quantité des données pouvant être stockée dans la mémoire tampon est élevée. Sélectionnez le type de vidéo à capturer à l'aide des options suivantes :
  - La mémoire tampon Console Capture (Capture console) permet de sélectionner le type de séquence de console à capturer. Vous pouvez activer une seule mémoire tampon ou les deux mémoires tampons simultanément. Les mémoires tampons partageant la même zone de données interne, l'activation des deux mémoires réduit la quantité de vidéo console pouvant être capturée. Afin d'optimiser l'utilisation des mémoires tampons, vous pouvez à tout moment en changer. Lorsque vous modifiez la configuration d'une mémoire tampon, les deux mémoires tampons sont réinitialisées et les informations contenues dans ces mêmes mémoires à ce moment-là sont perdues.
  - Auto Export/Fault Buffer (Export auto/Mémoire tampon fault) permet d'activer ou de désactiver automatiquement l'exportation des données de console capturées.
- Export Boot/Fault Buffer (Exporter mémoire tampon boot/fault) permet de spécifier l'emplacement URL d'un serveur Web qui accepte un transfert de données avec la méthode PUT ou POST. Par exemple : `http://192.168.1.1/images/capture%h%t.ilo` transfère les mémoires tampons de capture internes vers un serveur Web à l'adresse IP 192.168.1.1 et enregistre les données dans le dossier `images` sous le nom de fichier `captureServerNameDateTime-Boot (ou Fault).ilo`, où :
  - %h indique l'ajout du nom de serveur au nom de fichier.
  - %t indique qu'un horodatage sera inclus dans le nom de fichier.
  - Boot ou Fault est automatiquement ajouté pour désigner le type de mémoire tampon en tant qu'événement de séquence boot ou séquence fault.

    Pour plus d'informations sur la configuration du serveur Web et sur la procédure de configuration d'un serveur Web Apache en vue d'accepter les mémoires tampons de capture exportées, reportez-vous à la section « Configuration Apache - Acceptation de la mémoire

tampon de capture exportée » (Configuration Apache - Acceptation de la mémoire tampon de capture exportée à la page 225).

- ◦ Export (Exporter) permet de déclencher une exportation manuellement.
- ◦ Export username (Nom d'utilisateur export) correspond au nom d'utilisateur du serveur Web spécifié dans l'URL.
- ◦ Password (Mot de passe) correspond au mot de passe du serveur Web spécifié dans l'URL.

  Une fois les modifications apportées, cliquez sur **Apply** (Appliquer).

- Serial Port Configuration (Configuration du port série) affiche les paramètres courants des ports série du système et du port série virtuel. Les paramètres des ports série du système et du port série virtuel sont également affichés, indiquant les ports COM utilisés et les numéros IRQ.
- iLO 2 Virtual Serial Port (Port série virtuel iLO 2) affiche l'état courant de la connexion de ce port. Les modes suivants sont disponibles : en cours d'utilisation en mode brut ou en cours d'utilisation en mode normal. Si la connexion est en cours d'utilisation, le bouton Disconnect (Déconnecter) est disponible et peut être utilisé pour mettre fin à une connexion de port série virtuel. Le mode brut indique qu'un client est connecté à l'aide de l'utilitaire WiLODbg.exe servant au débogage distant du noyau Windows®.

Hot Keys (Touches d'activation) permet de définir des combinaisons de touches qui seront transmises au serveur hôte distant en appuyant sur une touche d'activation. Les touches d'activation de la console distante permettent d'envoyer des combinaisons de touches spécifiques, telles que Alt+Tab et Alt+Syst, de la session Java™ de la console distante au serveur. Pour plus d'informations, reportez-vous à la section « Touches d'activation de la console distante » (Touches d'activation de la console distante à la page 93).

Java affiche les spécifications Java™ requises pour chaque système d'exploitation pris en charge et un lien pour télécharger Java™. Pour plus d'informations, reportez-vous à la section « Navigateurs et systèmes d'exploitation client pris en charge » (Navigateurs et systèmes d'exploitation client pris en charge à la page 7).

Touches d'activation de la console distante

La page Program Remote Console Hot Keys (Touches d'activation de la console distante du programme) permet de définir jusqu'à six combinaisons de touches affectées à chaque touche d'activation. Lorsque vous appuyez sur une touche d'activation dans la console distante, au niveau des systèmes clients, la combinaison de touches définie (toutes les touches enfoncées simultanément) est transmise au serveur hôte distant à la place de la touche d'activation. Pour afficher les symboles accessibles à l'aide de la touche Alt Gr des claviers internationaux, définissez-les à l'aide de touches d'activation. Pour obtenir la liste des touches d'activation prises en charge, reportez-vous à la section « Touches d'activation prises en charge » (Touches d'activation prises en charge à la page 94).

Les touches d'activation de la console distante sont actives pendant une session de la console distante via l'IRC, l'applet de la console distante et pendant une session texte de la console distante via un client Telnet. Lorsque vous utilisez l'IRC, les états des voyants Verrouillage numérique, Verrouillage majuscule et Arrêt du défilement sur le clavier client ne reflètent pas obligatoirement l'état du clavier serveur. En revanche, l'activation de l'une de ces touches de verrouillage modifie l'état de verrouillage sur le serveur.

Pour définir une touche d'activation de la console distante :

1. Cliquez sur **Remote Console>Hot Keys** (Console distante>Touches d'activation).
2. Sélectionnez la touche d'activation à définir et utilisez les zones de liste déroulantes pour sélectionner la combinaison de touches à transmettre au serveur hôte au moment où vous appuyez sur la touche d'activation.
3. Cliquez sur **Save Hot Keys** (Enregistrer les touches d'activation) lorsque vous avez fini de définir les combinaisons de touches.

La page Program Remote Console Hot Keys (Touches d'activation de la console distante du programme) propose aussi l'option Reset Hot Keys (Réinitialiser touches d'activation). Cette option efface toutes les entrées des champs de touches d'activation. Cliquez sur **Save Hot Keys** (Enregistrer touches d'activation) pour enregistrer les champs effacés.

Touches d'activation prises en charge

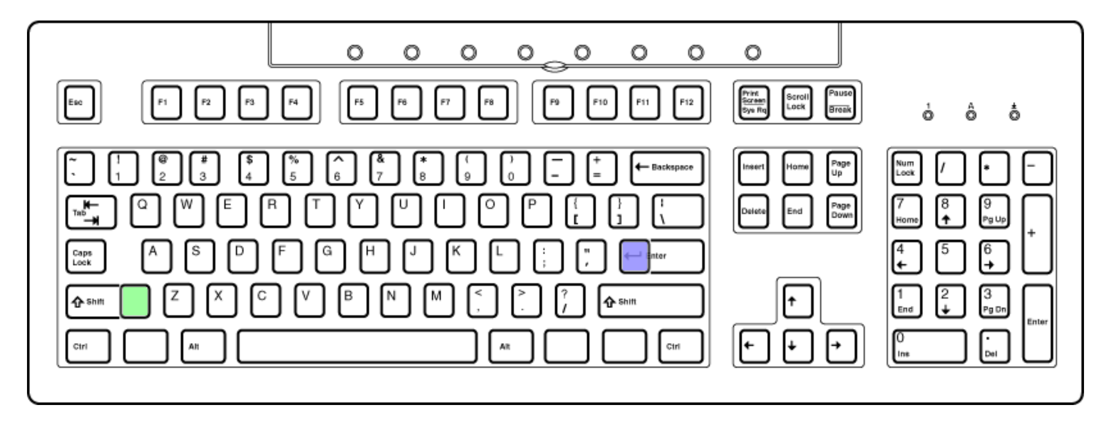
La page Program Remote Console Hot Keys (Touches d'activation de la console distante du programme) permet de définir jusqu'à 6 jeux différents de touches d'activation à utiliser durant une session de console distante. Chaque touche d'activation représente une combinaison de 5 touches différentes qui sont envoyées sur la machine hôte toutes les fois que vous appuyez sur une touche d'activation pendant une session de console distante. Les touches sélectionnées ainsi combinées (toutes les touches doivent être activées en même temps) sont transmises en une seule fois. Pour plus d'informations, reportez-vous à la section « Touches d'activation de la console distante » (Touches d'activation de la console distante à la page 93). Le tableau suivant dresse la liste de touches disponibles pour être utilisées dans les combinaisons de séquences de touches d'activation de la console distante.

ESC	F12	:	o
L_ALT	" " (Espace)	<	p
R_ALT	!	>	q
L_SHIFT (L_MAJ)	#	=	r
R_SHIFT (R_MAJ)	$	?	s
INS (INSER)	%	@	t
DEL (SUPPR)	&	[	u
HOME (ORIGINE)	~	]	v
END (Fin)	(	\	w
PG UP (PG PRÉC)	)	^	x
PG DN (PG SUIV)	*	_	y
ENTER (ENTRÉE)	+	a	z
TAB	-	b	{
BREAK	.	c	}
F1	/	d	|
F2	0	e	;
F3	1	f	'
F4	2	g	L_CTRL

F5	3	h	R_CTRL
F6	4	i	NUM PLUS
F7	5	j	NUM MINUS
F8	6	k	SCRL LCK (ARRÊT DÉFIL)
F9	7	l	BACKSPACE (RETOUR ARRIÈRE)
F10	8	m	SYS RQ
F11	9	n	

Touches d'activation et claviers internationaux

Pour définir des touches d'activation sur un clavier international, sélectionnez des touches de votre clavier dont les positions sont les mêmes sur un clavier américain. Pour créer une touche d'activation à l'aide de la touche internationale Alt Gr, utilisez R_ALT dans la liste des touches. Utilisez la disposition du clavier américain illustrée pour sélectionner vos touches.



Les touches colorées n'existent pas sur un clavier américain.

- La touche verte correspond aux symboles non américains \ et | sur un clavier international.
- La touche violette correspond aux symboles # et ~ non US sur un clavier international.

Touches d'activation et port série virtuel

Lorsque vous êtes connecté à la fonction Virtual Serial Port (Port série virtuel) de iLO 2 à l'aide de Telnet, la combinaison de touches CTRL+P+! (touche CTRL, touche P, touche MAJ et 1 touche appuyées simultanément) entraîne généralement le réamorçage du serveur distant.

Pour mettre le serveur distant hors tension, utilisez la combinaison de touches CTRL+P 6 et la combinaison de touches CTRL+P 1 pour le remettre sous tension.

Si iLO 2 ne répond pas, fermez la session Virtual Serial Port (Port série virtuel). iLO 2 se réinitialisera automatiquement au bout de 3 minutes environ et reviendra en mode de fonctionnement normal.

Mode plein écran de l'IRC

Le mode plein écran de l'option Integrated Remote Console (Console distante intégrée) permet de redimensionner le IRC afin qu'il présente la même résolution d'affichage que le système hôte distant. Pour revenir au bureau de votre système client, fermez la console.

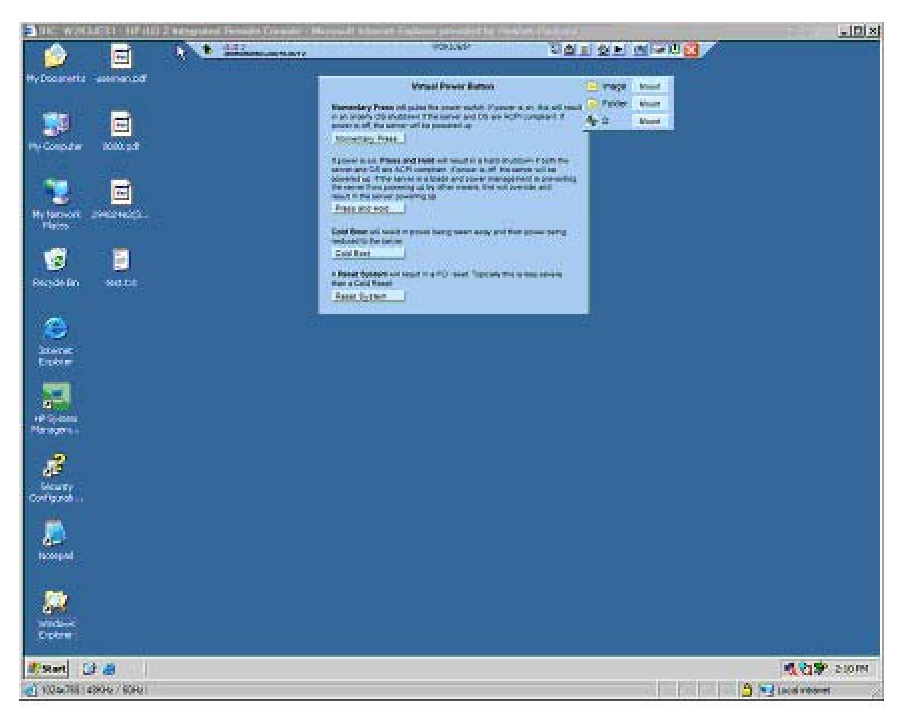
Le mode plein écran de l'option Integrated Remote Console (Console distante intégrée) a pour effet d'appliquer à votre système client la même résolution que celle du serveur distant. Le mode plein écran de l'option Integrated Remote Console (Console distante intégrée) tente de récupérer la meilleure configuration cliente pour cette résolution. Cependant, certains moniteurs peuvent rencontrer des problèmes si vous leur appliquez les fréquences d'actualisation les plus élevées prises en charge par l'adaptateur vidéo. Si tel est le cas, vérifiez les propriétés de votre bureau. Pour ce faire, cliquez avec le bouton droit sur le **bureau**, puis sélectionnez **Propriétés>Paramètres>Avancé>Écran** et choisissez une fréquence d'actualisation plus faible.

Pour plus d'informations sur l'affichage en plein écran de l'option Integrated Remote Console (Console distante intégrée), reportez-vous à la section « Option Integrated Remote Console (Console distante intégrée) » (Option Integrated Remote Console (Console distante intégrée) à la page 96).

Option Integrated Remote Console (Console distante intégrée)

L'option Integrated Remote Console (Console distante intégrée) offre une interface de console distante hautes performances pour clients Windows® et réunit les fonctions KVM, Virtual Power (Alimentation virtuelle) et Virtual Media (Support virtuel). Cette option est un contrôle ActiveX qui s'exécute à partir de Microsoft® Internet Explorer. Integrated Remote Console (Console distante intégrée) est une fonction sous licence disponible grâce à l'acquisition de licences supplémentaires. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21).

La console distante intégrée (IRC) prend en charge quatre sessions de console distante simultanées avec le même serveur si la fonction est activée via l'écran Remote Console Settings (Paramètres de la console distante), la CLI SMASH (OEM) ou RIBCL. Pour plus d'informations sur l'utilisation de plusieurs sessions de console distante, reportez-vous à la section « Console distante partagée » (Console distante partagée à la page 100).



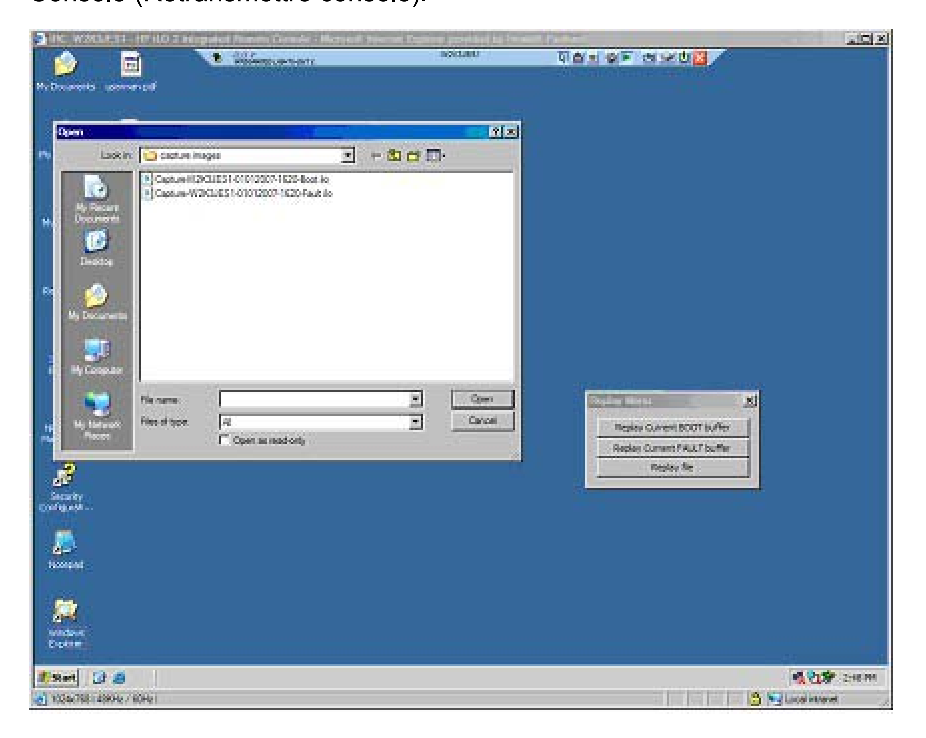
Integrated Remote Console (Console distante intégrée) et l'affichage Integrated Remote Console Fullscreen (Mode plein écran de la console distante intégrée) affichent une barre de menus et des boutons visibles à l'écran. La barre de menus présente les options suivantes :

- Remote Console Replay (Retransmission console distante) (icône lecture) : affiche la boîte de dialogue Replay Menu (Menu Retransmission) si Boot/Fault Console Capture (Capture console

boot/fault) est activé ou démarre la boîte de dialogue Open File (Ouvrir fichier) si Boot/Fault Console Capture (Capture console boot/fault) n'est pas activé.

◦ Replay Current BOOT buffer and Replay Current FAULT buffer (Retransmettre mémoire tampon BOOT en cours et Retransmettre mémoire tampon FAULT en cours) : permet de transférer les mémoires tampons capturées en interne vers le client à l'aide du port Console Replay (Retransmission console) spécifié dans l'onglet Administration>Access (Administration>Accès). Cliquez sur **Replay Current BOOT buffer** (Retransmettre mémoire tampon BOOT en cours) ou **Replay Current FAULT buffer** (Retransmettre mémoire tampon FAULT en cours) pour passer du menu Remote Console (Console distante) au menu Replay Console (Retransmettre console).

◦ Replay file (Retransmettre fichier) : affiche une boîte de dialogue Open (Ouvrir) permettant d'afficher un fichier précédemment enregistré. Après avoir sélectionné un fichier et cliqué sur **Open** (Ouvrir), le menu Remote Console (Console distante) se transforme en menu Replay Console (Retransmettre console).



- Replay (Retransmettre) (icône lecture sur le menu principal) : affiche l'option Replay Console (Retransmettre console). L'option Replay Console (Retransmettre console) fournit un contrôle sur la lecture de la mémoire tampon des données sélectionnée et affiche le temps de lecture écoulé.



La fonction Replay Console (Retransmettre console) présente les options suivantes :

- ◦ Cliquez sur **Play** (Lecture) pour commencer la lecture. Après avoir cliqué sur Play (Lecture) :

  — Cliquez sur **Pause** (Pause) pour arrêter la lecture et maintenir la position en cours. Pour reprendre la lecture, cliquez sur **Play** (Lecture) à partir de l'état en pause et la lecture reprend depuis la position en cours.

  — Cliquez sur **Stop** (Arrêter) pour interrompre la lecture et la reprendre au début de la mémoire tampon des données.

  — Cliquez sur **Fast-forward** (Avance rapide) pour augmenter la vitesse de lecture de 2, 4 ou 8 fois par rapport à la vitesse normale.

- ◦ Close (Fermer) apparaît lorsque la lecture est terminée. Cliquez sur **Close** (Fermer) pour quitter la fonction Replay Console (Retransmettre console) et afficher la barre de menus Remote Console (Console distante).

- Record (Enregistrer) (icône caméra) : permet d'enregistrer manuellement la vidéo en cours de la console du serveur. Cliquez sur **Record** (Enregistrer) pour afficher une boîte de dialogue Save (Enregistrer) et définir le nom de fichier et le répertoire dans lequel enregistrer la session en cours. Pendant une session d'enregistrement, le paramètre Record (Enregistrer) apparaît désactivé et passe au vert. Une fois activée, toute activité de la console du serveur apparaissant sur la console distante intégrée est enregistrée dans le fichier spécifié. Si vous cliquez sur **Record** (Enregistrer) pendant une session d'enregistrement, celle-ci s'arrête et le bouton Record (Enregistrer) revient à son état inactif normal. Pour lire l'enregistrement de nouveau, cliquez sur **Replay** (Retransmettre).
- Control (Contrôle) : permet au responsable de session d'exiger le contrôle complet si celui-ci a été autorisé pour un client satellite.
- Lock (Verrouiller) : permet d'empêcher toute requête de client satellite supplémentaire d'apparaître sur la console du leader de session.
- Client List (Liste de clients) : affiche le nom d'utilisateur et le nom DNS (si disponible) ou l'adresse IP des clients satellites actuels.
- Drive (Unité) : affiche tous les supports disponibles.
- Power (Alimentation) (icône d'alimentation verte) : affiche l'état de l'alimentation et permet d'accéder aux options d'alimentation. Le bouton Power (Alimentation) est de couleur verte lorsque le serveur est sous tension. Lorsque vous cliquez sur le bouton **Power** (Alimentation), l'écran Virtual Power Button (Bouton d'alimentation virtuelle) s'affiche avec quatre options : Momentary Press (Pression brève), Press and Hold (Pression prolongée), Cold Boot (Démarrage à froid du système) et Reset System (Réinitialiser le système).

  Lorsque vous appuyez sur le bouton Drives (Lecteurs) ou le bouton Power (Alimentation), le menu qui s'affiche reste ouvert même lorsque vous déplacez la souris en dehors de la barre de menus.
- CAD (Ctrl-Alt-Suppr) : permet de démarrer une boîte de dialogue pour envoyer les touches Ctrl-Alt-Suppr (ou n'importe laquelle des six touches d'activation) au serveur.
- Thumb tack (Punaise) : permet de garder ouvert le menu principal de la console distante ou de réduire le menu principal lorsque le curseur de la souris s'éloigne.
- Exit (Quitter) (icône X rouge) : permet de fermer et quitter la console distante.

Les améliorations de sécurité Internet Explorer 7 affichent la barre d'adresse dans toute fenêtre récemment ouverte. Pour supprimer la barre d'adresse de l'IRC, vous devez modifier le niveau par défaut du paramètre Security (Sécurité). Pour supprimer la barre d'adresse, définissez « Allow websites to open windows without address or status bars » (Autoriser les sites Web à ouvrir les fenêtres sans barre d'adresse ou d'état » sur **Enable** (Activer).

Optimisation des performances de la souris pour les fonctions Remote Console (Console distante) ou Integrated Remote Console (Console distante intégrée)

Dans certaines configurations Microsoft® Windows®, l'accélération de la souris doit être définie de façon à ce que la souris de la console distante puisse être correctement maniée.

SLES 9

Choisissez la souris correspondant à la souris de la console distante à l'aide de la commande `xsetpointer -l` qui permet de répertorier toutes les souris.

1. Choisissez la souris à modifier en comparant la sortie de xsetpointer à la configuration de X (/etc/X11/XF86Config ou /etc/X11/xorg.conf).
2. Sélectionnez la souris de la console distante comme correspondant à la souris que vous souhaitez modifier. Par exemple :

   ```
   xsetpointer Mouse[2]
   ```

3. Définissez les paramètres d'accélération. Par exemple :

   ```
   xset m 1/1 1
   ```

Red Hat Enterprise Linux

Définissez les paramètres d'accélération à l'aide de :

```
xset m 1/1 1
```

Synchronisation de la souris de Windows®

Le paramètre High Performance Mouse (Souris hautes performances) par défaut de la page Global Settings (Paramètres généraux) a été conçue pour utiliser le paramètre le plus performant du système d'exploitation du serveur. Cette fonction nécessite que le driver d'interface de supervision HP ProLiant Lights-Out soit chargé et que le serveur ait été relancé après l'installation du driver. Si vous rencontrez des problèmes de synchronisation de la souris sous Windows, définissez le paramètre High Performance Mouse (Souris hautes performances) sur **Yes** (Oui).

Paramètres High Performance Mouse (Souris hautes performances)

Lorsque vous utilisez la console distante, vous pouvez activer la fonction High Performance Mouse (Souris hautes performances). Cette fonction améliore considérablement la performance et la précision du pointeur sur les systèmes d'exploitation pris en charge. High Performance Mouse (Souris hautes performances) de iLO 2 est un dispositif de pointage qui fournit des coordonnées de position exactes pour décrire son emplacement comme une tablette souris USB. Une souris classique envoie des informations de position relatives (par exemple, déplacement de la souris de 12 pixels vers la droite). L'ordinateur hôte peut modifier les informations de position relatives pour activer des fonctions comme l'accélération de la souris. Lorsqu'il utilise la console distante, le client n'est pas conscient de ces modifications. Par conséquent, la synchronisation entre le curseur de la souris client et le curseur de la souris hôte échoue.

Les applets Integrated Remote Console (Console distante intégrée) et Remote Console (Console distante) envoient des coordonnées de curseur de souris absolues et relatives à iLO 2. Lorsque iLO 2 est en mode High Performance Mouse (Souris hautes performances), il ignore les coordonnées relatives et envoie les coordonnées absolues à l'émulateur de tablette souris USB. Le serveur « voit » alors la souris se déplacer comme si les informations de coordonnées provenaient d'une tablette souris USB locale. Lorsque iLO 2 n'est pas en mode High Performance Mouse (Souris hautes performances), les coordonnées absolues et les coordonnées relatives sont envoyées à l'émulateur de souris USB relative.

La fonction High-Performance Mouse (Souris hautes performances) n'est prise en charge que sur les systèmes d'exploitation prenant en charge une tablette souris USB. Les utilisateurs de Windows®

peuvent activer l'option High Performance Mouse à l'écran Remote Console Settings. Les utilisateurs de Linux doivent activer l'option High Performance Mouse (Souris hautes performances) une fois que la souris hautes performances iLO 2 du driver Linux est installée. Les serveurs utilisant un autre système d'exploitation qui rencontrent des problèmes avec la souris de la console distante doivent désactiver cette option.

Lorsque vous utilisez l'option Integrated Remote Console (Console distante intégrée) depuis iLO 2 et SmartStart, les souris locale et distante ne restent pas alignées. Le paramètre High Performance Mouse doit être désactivé lorsque vous utilisez SmartStart. Si les souris perdent l'alignement alors que vous utilisez la fonction High Performance Mouse, la touche Ctrl située à droite permet de les réaligner. Vous avez également le choix d'utiliser la console distante Java™ au lieu de la console distante intégrée.

L'option High Performance Mouse minimise tous les problèmes de synchronisation de souris sur les systèmes d'exploitation hôtes pris en charge. Vous pouvez sélectionnez ce mode à la page Remote Console Settings avant le démarrage d'une console distante. Il n'est cependant pas pris en charge par tous les systèmes d'exploitation, en particulier lors de l'installation. Pour obtenir les meilleures performances :

- Sélectionnez une résolution d'écran de serveur distant inférieure pour améliorer les performances de la console distante. La résolution maximum prise en charge est 1280 x 1024 pixels.
- Définissez une résolution d'écran client supérieure à celle du serveur distant pour optimiser la visibilité de la console distante.
- La qualité de la couleur du serveur distant est sans effet sur les performances de la console distante. Le rendu de celle-ci est en 4096 couleurs (12 bits).
- Utilisez un pointeur de souris non animé sur le système distant.
- Désactivez l'ombre de la souris sur le système distant.

Pour configurer le serveur hôte, réglez les paramètres suivants du Panneau de configuration :

1. Sélectionnez **Souris>Pointeurs>Modèle>Windows par défaut**. Cliquez sur **OK**.
2. Dans la page Souris>Pointeurs, sélectionnez **Activer l'ombre du pointeur**. Cliquez sur **OK**.
3. Sélectionnez **Affichage>Paramètres>Avancé>Dépannage>Accélération matérielle>Complète**. Cliquez sur **OK**.
4. Sélectionnez **Système>Avancé>Paramètres de performances>Effets visuels>Ajuster afin d'obtenir les meilleures performances**. Cliquez sur **OK**.

Sinon, l'utilitaire de configuration en ligne HP (HPONCFG) peut automatiquement régler ces paramètres. Vous pouvez également modifier les paramètres de la fonctionnalité High Performance Mouse (Souris hautes performances) à l'aide de la commande XML `MOD_GLOBAL_SETTINGS`. Pour plus d'informations sur l'utilisation de la commande RIBCL `MOD_GLOBAL_SETTINGS`, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Console distante partagée

Shared Remote Console (Console distante partagée) est une fonction iLO 2 qui permet de se connecter à quatre sessions maximum sur le même serveur. Cette fonction ne remplace par la fonction Acquire (Acquérir) décrite à la section « Acquisition de console distante » (Acquisition de la console distante à la page 104) ni n'autorise les clients à accès intégral (lecture/écriture) à contrôler l'alimentation. Une console distante partagée ne prend pas en charge la transmission d'une désignation de serveur hôte à un autre utilisateur ni le rétablissement d'une connexion utilisateur échouée après une panne. Pour autoriser un accès à l'utilisateur après une panne, vous devez redémarrer la session de console distante.

Shared Remote Console (Console distante partagée) est une fonction sous licence disponible grâce à l'acquisition de licences supplémentaires. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21).

Shared Remote Console (Console distante partagée) et le mode Forced Switch (Commutation forcée) sont désactivés par défaut. Vous devez activer et configurer ces fonctions via le navigateur, la CLI SMASH(OEM) ou RIBCL. Toutes les sessions de console sont cryptées en authentifiant le client d'abord, puis le leader de session décide d'autoriser ou pas la nouvelle connexion.

Le premier utilisateur à initier une session de console distante se connecte normalement au serveur et est désigné comme leader de session (hôte de session.) Tout utilisateur suivant demandant l'accès à la console distante initie une demande d'accès, laquelle exige une connexion de client satellite et le recours au leader de session. Une fenêtre contextuelle pour chaque demande de client satellite apparaît sur le bureau du leader de session pour identifier le nom d'utilisateur et le nom DNS (si disponible) ou l'adresse IP du demandeur.

Les hôtes de session sont libres d'accorder ou de refuser l'accès. Une liste d'utilisateurs et des noms d'hôtes de session apparaît dans le cadre du navigateur de la console distante. Les sessions des clients satellites prennent fin quand l'hôte de session a terminé.

Les sessions partagées ne fonctionnent pas bien avec les fonctions de capture et de retransmission de console de iLO 2. Si une session satellite visualise une session capturée, pendant la durée de la lecture, la session satellite ne reçoit pas de messages de contrôle du leader de session. Si un hôte de session commence à visualiser des données vidéo capturées pendant une session partagée, la vidéo est affichée sur toutes les sessions satellites de la console distante.

Utilisation de la fonction Console Capture (Capture console)

Console Capture (Capture console) est une fonction de console distante qui permet d'enregistrer et retransmettre un flux vidéo d'événements comme l'amorçage, les événements ASR et les erreurs détectées dans le système d'exploitation. Vous pouvez également démarrer et arrêter manuellement l'enregistrement de la vidéo de console. Console Capture (Capture console) n'est disponible que par le biais de l'interface utilisateur iLO 2 et n'est pas accessible via la création de scripts XML ou le CLP. Console Capture (Capture console) est une fonction sous licence disponible grâce à l'acquisition de licences supplémentaires. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21).

Une zone de mémoire tampon est réservée dans le processeur de supervision pour stocker les données vidéo capturées. Cette zone de mémoire tampon est partagée avec la mémoire tampon de mise à jour du microprogramme, si bien que toute information capturée est perdue quand vous lancez le processus de mise à jour du microprogramme. Vous ne pouvez pas capturer de données vidéo pendant le processus de mise à jour du microprogramme.

L'espace de la mémoire tampon est limité. Un seul type d'événement à la fois est stocké dans la zone de mémoire tampon. Vous pouvez transférer des mémoires tampons contenant des données capturées vers un client exécutant l'IRC pour la retransmission. Vous pouvez également configurer le système iLO 2 pour qu'il envoie automatiquement les données vidéo capturées à un serveur Web sur le même réseau que lui lorsqu'un événement se produit. Le serveur Web doit accepter les transferts de données avec la méthode POST. Vous pouvez sélectionner Boot buffer (Mémoire tampon boot) uniquement, Fault buffer (Mémoire tampon fault) ou combiner les deux sous forme de large mémoire tampon pour disposer de plus d'espace pour capturer les séquences boot Linux.

Les données de mémoire tampon exportées sont affectées d'un nom unique afin de faciliter leur identification pour la retransmission. La retransmission nécessite un système iLO 2 sous licence sur le réseau. Certains systèmes d'exploitation (comme Linux) peuvent remplir la mémoire tampon rapidement. En laissant la console système en mode texte, vous optimisez la quantité des informations capturées. En outre, en fermant ou en réduisant le nombre d'éléments de console graphiques actifs, vous optimisez l'espace de mémoire tampon interne.

Vous pouvez manuellement capturer la vidéo de la console serveur à l'aide de la fonction IRC Record (Enregistrement IRC). Toutes les données manuellement capturées sont stockées dans un fichier local sur le client pour une retransmission future.

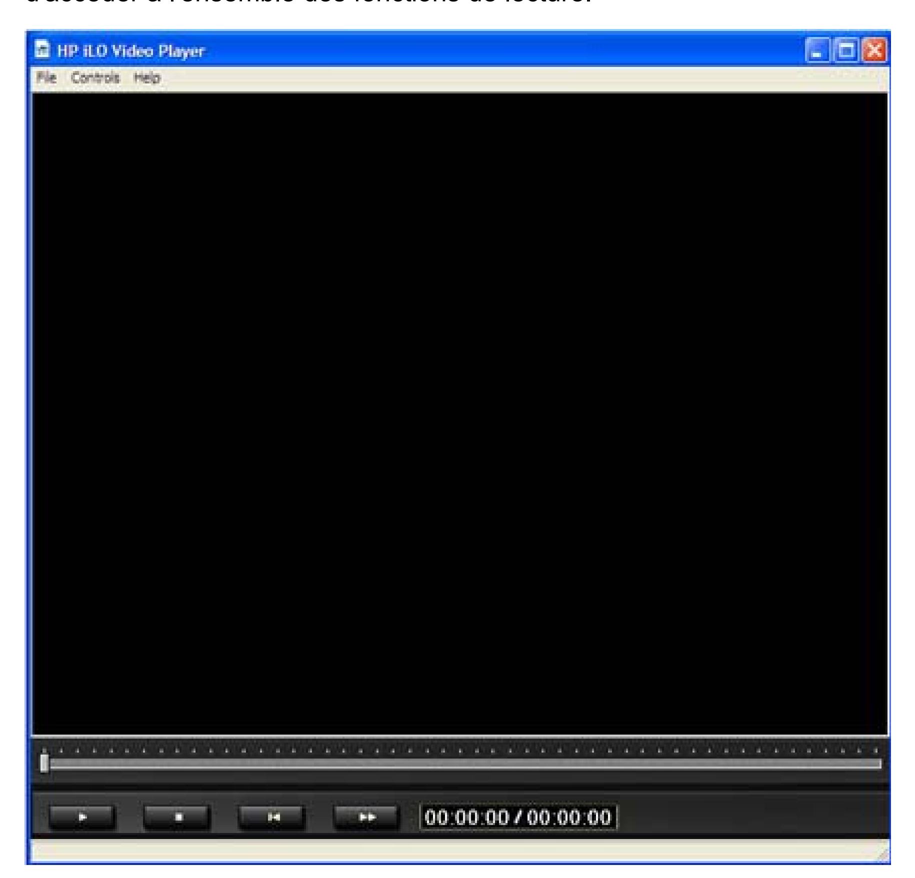
Utilisation de HP iLO Video Player

HP iLO Video Player vous permet de lire les fichiers de capture de la console iLO 2 sans qu'il soit nécessaire d'installer la carte iLO 2 sur le système local. Ce lecteur se présente sous la même forme qu'un lecteur multimédia classique et propose des commandes similaires. Vous pouvez exécuter HP iLO Video Player en tant qu'application autonome sur un serveur ou un client. Généralement, l'application réside sur le client. Quant aux fichiers de capture iLO 2, ils sont créés à l'aide de la fonction iLO 2 Console Capture (Capture console). Pour plus d'informations, reportez-vous à la section « Utilisation de la fonction Console Capture (Capture console) » (Utilisation de la fonction Console Capture (Capture console) à la page 101).

Pour pouvoir utiliser HP iLO Video Player, vous devez disposer du système d'exploitation Microsoft Windows® 2000, Windows® XP ou Windows Vista®, et Internet Explorer (version 6 ou ultérieure) doit être installé sur le système.

Interface utilisateur de HP iLO Video Player

Lorsque vous lancez HP iLO Video Player, l'interface utilisateur de l'application apparaît et vous permet d'accéder à l'ensemble des fonctions de lecture.



HP iLO Video Player propose les options de menu suivantes :

- File (Fichier)
  - Open (Ouvrir) : ouvre un fichier de capture vidéo.
  - Exit (Quitter) : ferme HP iLO Video Player.
- Controls (Commandes)
  - Play (Lire) : lit le fichier de capture vidéo actif ou reprend la lecture.
  - Stop (Arrêter) : interrompt la lecture du fichier de capture vidéo actif.
  - Skip to Start (Revenir au début) : redémarre la lecture du fichier de capture vidéo actif.
  - Change Speed (Modifier la vitesse) : change la vitesse de lecture du fichier de capture vidéo iLO actif.
- Aide
  - Help Topics (Rubriques d'aide) : ouvre le fichier d'aide HP iLO Video Player.
  - About (À propos de) : ouvre la page iLO Video Player About (À propos d'iLO Video Player).

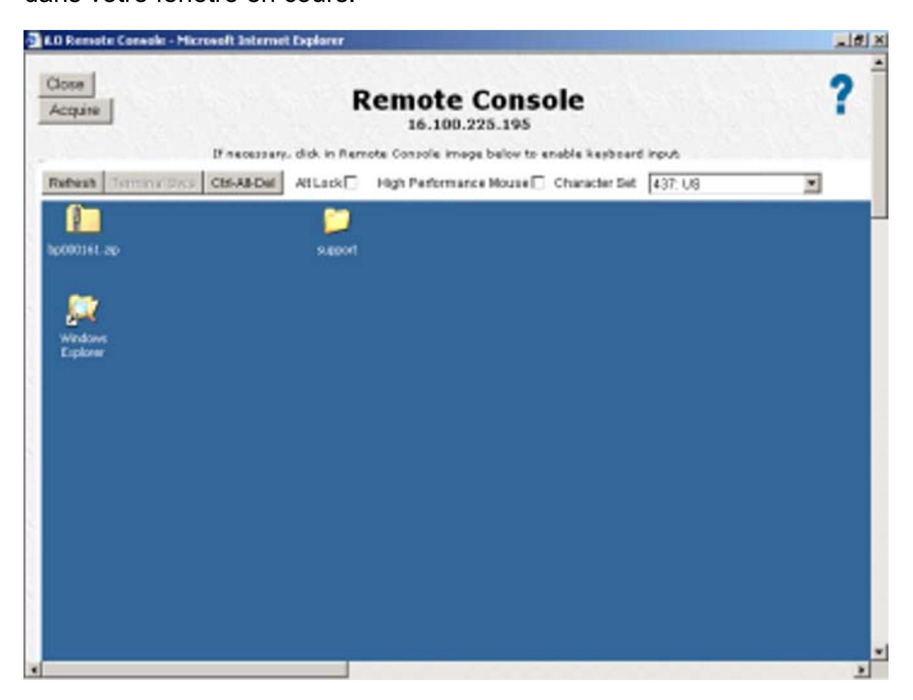
Commandes HP iLO Video Player

Commande	Nom	Fonction
	Play/Pause (Lire/Pause)	Démarre la lecture du fichier sélectionné si ce n'est pas déjà le cas ou si elle a été mise en pause. Utilisez cette commande en cours de lecture pour mettre le fichier en pause. Lorsqu'aucun fichier n'est sélectionné, le bouton est désactivé.
	Stop (Arrêter)	Arrête la lecture. Lorsqu'aucun fichier n'est sélectionné, le bouton est désactivé.
	Skip to Start (Revenir au début)	Redémarre la lecture à partir du début du fichier. Lorsqu'aucun fichier n'est sélectionné, le bouton est désactivé.
	Seek (Rechercher)	Permet d'avancer ou de revenir en arrière. Lorsqu'aucun fichier n'est sélectionné, le bouton est désactivé.

Commande	Nom	Fonction
	Change Speed (Modifier la vitesse)	Change la vitesse de lecture du fichier sélectionné. La vitesse peut être augmentée de 2, 4, 8 ou 16 fois. Appuyez de manière successive sur ce bouton pour multiplier la vitesse par 2, 4, 8, 16 fois, puis 1 fois (vitesse normale). Lorsqu'aucun fichier n'est sélectionné, le bouton est désactivé.
00:00:00 / 00:00:00	File Position (Position dans le fichier)	Affiche les paramètres de durée du fichier sélectionné, au format HH:MM:SS. • La valeur de gauche indique la position à laquelle vous vous trouvez dans le fichier. • La valeur de droite correspond à la durée totale du fichier.

Acquisition de la console distante

Lorsque le paramètre Remote Console Acquire (Acquisition de la console distante) de l'écran Remote Console Settings (Paramètres de la console distante) est activé, la page Remote Console comporte le bouton Acquire (Acquérir). Si vous avez ouvert cette dernière et êtes alors informé qu'un autre utilisateur est en train d'utiliser la console distante, l'action de cliquer sur le bouton Acquire (Acquérir) mettra fin à la session de console distante de l'utilisateur en question et démarrera une session de console distante dans votre fenêtre en cours.



Lorsque vous cliquez sur Acquire (Acquérir), vous êtes invité à confirmer que vous souhaitez interrompre la session de l'utilisateur tiers. Ce dernier reçoit alors un avertissement l'informant qu'un tiers a acquis la session de console distante après avoir perdu la connexion. Aucun avertissement préalable n'est émis. Une fois que vous avez confirmé que vous souhaitez poursuivre l'opération d'acquisition, vous êtes informé, par une fenêtre d'alerte, que l'opération peut prendre 30 secondes ou

plus pour être réalisée. Le bouton Acquire (Acquérir) est désactivé une fois que vous avez appuyé dessus et l'opération d'acquisition démarre. Sur les navigateurs qui le prennent en charge, le bouton prend une couleur gris clair pour indiquer qu'il est désactivé. Sur d'autres navigateurs, rien n'indique qu'il est désactivé.

Seule une commande Acquire (Acquérir) est autorisée par utilisateur et par période de cinq minutes. Si un autre utilisateur a récemment acquis la console distante, le fait de cliquer sur le bouton Acquire (Acquérir) peut générer une page vous informant que la période de désactivation de l'acquisition de cinq minutes est en vigueur. Fermez la fenêtre et relancez la console distante. Le bouton Acquire (Acquérir) est désactivé dans la nouvelle page jusqu'à expiration de la période désactivation de l'acquisition. Lorsque le bouton Acquire (Acquérir) est activé (cela se produit automatiquement, vous n'avez pas besoin de rafraîchir la page), vous pouvez tenter d'acquérir à nouveau la console distante. Sur les navigateurs qui le prennent en charge, le bouton prend une couleur gris clair pour indiquer qu'il est désactivé pendant cette période de cinq minutes. Sur d'autres navigateurs, rien n'indique que le bouton est désactivé. Vous ne disposez donc d'aucun repère visuel pour vous prévenir de la fin du délai d'attente.

Une seule tentative d'acquisition peut être effectuée par fenêtre de session de console distante. Si vous êtes parvenu à acquérir la console distante et que quelqu'un l'acquiert à son tour à vos dépens, vous devez ouvrir une nouvelle fenêtre de console distante afin de tenter d'en acquérir une nouvelle session.

Remote Console (Console distante)

Remote Console (Console distante) est une applet Java™ qui permet d'accéder à la console distante depuis une gamme étendue de navigateurs, notamment Windows® et Linux. Les navigateurs pris en charge sont répertoriés dans la section « Navigateurs et systèmes d'exploitation client pris en charge » (Navigateurs et systèmes d'exploitation client pris en charge à la page 7). Remote Console (Console distante) est une fonction sous licence disponible grâce à l'acquisition de licences supplémentaires. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21).



La console distante utilise des curseurs doubles pour faciliter la distinction entre le pointeur de la souris locale et celui de la souris distante. Le curseur de la souris de l'ordinateur client apparaît sur la console distante sous forme de croix. Pour des performances optimales, vérifiez que l'écran du système hôte est configuré conformément aux instructions fournies dans les sections « Paramètres client

recommandés » (Paramètres client recommandés à la page 106) et « Paramètres serveur recommandés » (Paramètres serveur recommandés à la page 107).

Pour synchroniser les curseurs distant et local en cas de non alignement, procédez ainsi :

- Cliquez sur le bouton droit de la souris et déplacez le pointeur local afin de le ramener vers le curseur de la souris du serveur distant.
- Tout en maintenant la touche **Ctrl** (située à droite) enfoncée, amenez le curseur local en forme de croix sur le curseur du serveur distant.

Le curseur local prend la forme du curseur distant. Le curseur s'affiche sous la forme d'un curseur simple si le curseur local et le curseur distant s'alignent parfaitement et que l'accélérateur est défini à Full (Complet) sur le serveur géré.

Fonctions et commandes de la console distante

L'applet Remote Console (Console distante) présente des boutons qui fournissent à iLO 2 des fonctions et des commandes améliorées. Ces options sont :

- Refresh (Actualiser) permet le rafraîchissement de l'écran par iLO 2.
- Terminal Svcs (Svsc Terminal) lance le client Microsoft® Terminal Services (Services Terminal) installé sur le système. Ce bouton est désactivé si la fonction Terminal Services (Services Terminal) est désactivée ou non installée sur le serveur.
- Ctrl-Alt-Del (Ctrl+Alt+Suppr) permet d'entrer cette combinaison de touches dans la console distante.
- Alt Lock (ALt Verr) permet d'envoyer n'importe quelle touche activée au serveur comme si vous aviez appuyé simultanément sur la touche Alt et une autre touche.
- Character Set (Jeu de caractères) modifie le jeu de caractères défini utilisé par la console distante. La modification du jeu de caractères de la console distante garantit l'affichage correct des caractères.
- Close (Fermer) permet de mettre fin à la session de console distante et de fermer la fenêtre de la console distante.

Paramètres client recommandés

Dans l'idéal, il convient que la résolution d'affichage du système d'exploitation du serveur distant soit égale ou inférieure à celle de l'ordinateur qui le consulte. Une résolution de serveur supérieure permet de transmettre plus d'informations, mais ralentit les performances générales.

Utilisez les paramètres suivants pour le client et le navigateur, de façon à optimiser les performances :

- **Propriétés d'affichage**
  - Choisissez une résolution d'écran supérieure à 256 couleurs.
  - Choisissez une résolution d'écran supérieure à celle du serveur distant.
  - Propriétés d'affichage de Linux X : dans l'écran X Preferences (Préférences X), paramétrez la taille de la police sur **12**.
- **Remote Console (Console distante)**
  - Pour la vitesse de la console distante, il est conseillé d'utiliser un client de 700 MHz ou plus rapide, avec 128 Mo de mémoire minimum.
  - Pour l'exécution de l'applet Java™ Remote Console, HP recommande d'utiliser un client à processeur unique.
- **Propriétés de la souris**
  - Réglez le paramètre Mouse Pointer (Pointeur de la souris) sur une vitesse moyenne.
  - Réglez le paramètre Mouse Pointer Acceleration (Accélération du pointeur) sur une valeur faible ou désactivez-le.

Paramètres serveur recommandés

La liste ci-dessous indique les paramètres recommandés pour les serveurs en fonction des différents systèmes d'exploitation.

REMARQUE : pour afficher entièrement l'écran du serveur hôte sur l'applet de la console distante du client, paramétrez l'écran du serveur sur une résolution inférieure ou égale à celle du client.

Paramètres de Microsoft® Windows® Server 2003

Pour optimiser les performances, choisissez un arrière-plan uni dans l'option **Display Properties** (Propriétés d'affichage) du serveur (pas de papier peint à motifs) et, dans l'option **Mouse Properties** (Propriétés de la souris) pour le serveur, choisissez **Disable Pointer Trails** (Désactiver l'ombre de la souris).

Paramètres des serveurs Red Hat Linux et SUSE Linux

Pour optimiser les performances, définissez l'option Mouse Properties>Pointer Acceleration (Propriétés de la souris>Accélération du pointeur) sur **1x**. Pour KDE, accédez au panneau **KDE Control Center** (Centre de contrôle KDE), sélectionnez **Peripherals/Mouse** (Périphériques/Souris), puis cliquez sur l'onglet **Advanced** (Avancé).

Présentation de la console distante texte

iLO ainsi que ses prédécesseurs prennent en charge une véritable console distante texte. Les informations concernant la vidéo sont obtenues à partir du serveur. Le contenu de la vidéo est envoyé au processeur de supervision, puis compressé, codé et envoyé à l'application cliente de supervision. iLO utilise une mémoire tampon d'écran qui détecte les modifications des informations du texte, les code et envoie les caractères (y compris les informations de positionnement de l'écran) aux applications clientes texte. Cette méthode est compatible avec les clients texte standard, performante et simple. Cependant, vous ne pouvez pas afficher d'informations graphiques ou non-ASCII. Les informations sur le positionnement de l'écran (caractères affichés) peuvent être erronées.

La console distante utilise Virtual KVM et ne propose pas de véritable console texte. iLO 2 utilise le port DVO d'adaptateur vidéo pour accéder directement à la mémoire vidéo. Cette méthode augmente de

manière significative les performances de iLO 2. Cependant, le flux vidéo numérique ne contient pas de données texte utiles. Les données obtenues par le port DVO représentent les données graphiques (non basées sur les caractères) et ne sont pas des données ASCII ou texte intelligibles. Ces données vidéo ne peuvent pas être traitées par une application cliente texte telle que Telnet ou SSH.

Console texte pendant le POST

La console distante texte iLO 2 standard reste disponible jusqu'à la fin de la séquence POST du système d'exploitation. Le microprogramme iLO 2 standard continue d'utiliser la fonctionnalité de port série virtuel du processeur de supervision. Dans le microprogramme iLO 2, le port série virtuel s'appelle Remote Serial Console (Console série distante). iLO 2 utilise cette console série distante pour accéder à une console distante texte avec pré-système d'exploitation. L'applet iLO 2 Remote Serial Console s'affiche sous la forme d'une console texte, mais les informations sont représentées à l'aide de données vidéo graphiques. iLO 2 affiche ces informations au moyen de l'applet de console distante lorsque le serveur se trouve à l'état de pré-système d'exploitation, permettant ainsi à une carte iLO 2 sans licence d'observer le serveur et d'interagir avec lui lors des séquences POST.

Pour une lame iLO 2 (et une lame iLO exécutant Linux sous un format graphique), entrez `getty()` sur le port série du serveur, puis utilisez la console série distante iLO 2 ou le port série virtuel iLO (commande CLP `start /system1/oemhp_vsp1`) pour observer une session sur le système d'exploitation Linux via le port série.

Une carte iLO 2 sans licence ne peut plus accéder à la console distante une fois que le serveur a terminé le POST et que le chargement du système d'exploitation a commencé. Pour pouvoir utiliser les fonctions Remote Console (Console distante) et iLO Text Console after POST (Console texte après le POST), vous devez disposer d'un pack iLO 2 Advanced ou iLO 2 Advanced pour BladeSystem.

Console texte après le POST

La fonction iLO Text Console after POST (Console texte après le POST) est une console texte accessible via telnet ou SSH après la séquence POST. Lorsque vous utilisez SSH, le flux de données, y compris les informations d'authentification, est protégé par une méthode de codage prise en charge par le client SSH et par iLO 2. HP conseille d'utiliser un client SSH pour se connecter à la console texte iLO.

Il est également possible de se connecter à la console texte iLO 2 depuis un client telnet. Sachez cependant que lorsque vous utilisez une connexion telnet classique, le flux de données n'est pas codé. Dans la stratégie de sécurité par défaut, telnet est désactivé. Vous devez activer telnet pour autoriser l'accès à l'interface CLI et à la console texte iLO 2.

Pour plus d'informations sur la sécurité des méthodes de communication employés par iLO 2, reportez-vous au document *Integrated Lights-Out security technology brief* (Sécurité de HP Integrated Lights-Out, présentation de la technologie) disponible sur le site Web HP (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00212796/c00212796.pdf).

La façon dont les couleurs, les caractères et les commandes s'affichent à l'écran varie en fonction du client. Vous pouvez choisir n'importe quel client telnet (si activé) ou SSH standard compatible avec iLO 2. La console texte iLO 2 est activée par défaut pour les versions 1.50 et ultérieures du microprogramme iLO 2. Elle présente les caractéristiques suivantes :

- Écrans d'affichage en mode texte de 80 x 25 (configurations couleur standard) lorsque le système est lancé, avec :
  - Processus d'amorçage du système (POST)
  - Option ROM standard
  - Chargeurs boot texte (LILO ou GRUB)

    - Système d'exploitation Linux en mode VGA 80 x 25
    - DOS
    - Autres systèmes d'exploitation de type texte

      L'écran en mode texte ne prend pas en charge les éléments suivants : graphiques, autres résolutions texte VGA (132 x 48, 80 x 48) et autres résolutions texte appliquées au moyen d'un driver (appliquées graphiquement).
- Touches d'activation de la console distante
- Claviers en langue internationale (lorsque le serveur et le client respectent la même configuration)
- Caractères de tracé, lorsque la police et la page de code appropriées sont sélectionnées dans l'application cliente

Pour pouvoir utiliser la console texte iLO 2, vous devez nécessairement mettre à jour la ROM hôte. Cette console est prise en charge par iLO 2 sur les serveurs HP ProLiant BL460c G1, BL480c G1, ML350 G5, DL360 G5, ML370 G5, DL380 G5, BL680 G5 et DL580 G5.

Utilisation de la console texte iLO

Pour lancer une session de console texte iLO 2 :

1. Démarrez une session SSH ou telnet.

   Vérifiez que les caractères de l'application du terminal sont codés en Western (ISO-8859-1).
2. Connectez-vous à la carte iLO 2.
3. À l'invite, entrez la commande `textcons`.

   Un message s'affiche et indique que le logiciel de la console texte iLO 2 est en cours d'initialisation.

Pour quitter la console texte iLO et revenir à la session CLI, utilisez la combinaison de touches **ESC (**.

Personnalisation de la console texte iLO 2

Lors du démarrage de la console texte iLO 2, vous pouvez utiliser les options et arguments de la commande `textcons` afin de personnaliser le fonctionnement de l'écran. En général, vous n'avez pas à changer ces options.

- Contrôle de la fréquence d'échantillonnage

  Utilisez l'option `textcons speed` pour définir le laps de temps séparant deux périodes d'échantillonnage (valeur exprimée en millisecondes). La période d'échantillonnage correspond au temps requis par le microprogramme pour analyser les modifications relatives à l'affichage et mettre à jour la console texte iLO 2. En ajustant la vitesse, vous pouvez soulager le trafic sur les liaisons réseau lentes ou longue distance, réduire la bande passante consommée et limiter l'utilisation de l'UC iLO 2. Les valeurs raisonnables sont comprises entre 1 et 5 000 (1 ms à 5 s). Par exemple :

  ```
  textcons speed 500
  ```

- Contrôle du lissage

  iLO 2 tente uniquement d'envoyer des données lorsque celles-ci changent et s'affichent de façon stable à l'écran. Lorsqu'une ligne de l'écran texte change en permanence et de façon trop rapide, iLO 2 attend qu'elle soit stabilisée pour pouvoir l'envoyer. Par exemple, lorsque la commande `ls -R` est exécutée sur un système de fichiers volumineux, le texte s'affiche trop rapidement sur l'écran physique et ne peut pas être interprété. Il en est de même pour les sessions de la console texte iLO 2. Les données s'affichent trop rapidement et il est impossible de les déchiffrer. Cela n'empêche pas que les données sont envoyées par iLO 2 sur le réseau, consommant ainsi de la bande de passante. Le lissage est activé par défaut (retard de 0), de sorte que seuls les changements stabilisés à l'écran sont envoyés. Vous pouvez contrôler ou désactiver le lissage à l'aide de l'option delay. Par exemple :

  ```
  textcons speed 500 delay 10
  ```

- Contrôle de la prise en charge du clavier international

  Lorsque la console texte iLO 2 est utilisée, iLO 2 peut émuler une correspondance de caractères entre le client, telnet et le serveur. La correspondance par défaut correspond à la conversion (ou non-conversion) du clavier 101 USB.

  Pour contrôler la conversion, utilisez l'option `xlt`, suivie de la référence appropriée. Par exemple, pour appliquer une fréquence d'échantillonnage de 50 ms avec un clavier britannique, entrez :

  ```
  textcons speed 50 xlt 41
  ```

  Pour convertir le clavier vers une autre langue, reportez-vous au tableau suivant :

Clavier	Référence
Anglais (États-Unis)	0
British (Anglais - Grande-Bretagne)	1
Belgian (Français - Belgique)	2
Danish (Danois)	3
Finnish (Finlandais)	4
Français	5
French Canadian (Français - Canada)	6

Clavier	Référence
German (Allemand)	7
Italian (Italien)	8
Latin American (Espagnol -Amérique latine)	9
Norvégien	10
Portuguese (Portugais)	11
Spanish (Espagnol)	12
Swedish (Suédois)	13
Français (Suisse)	14
Allemand (Suisse)	16

- Configuration des touches d'activation de la console distante

  Les touches d'activation configurées pour la console distante fonctionnent dans la console texte iLO 2 et permettent d'utiliser des séquences de touches spéciales qu'il est impossible de dupliquer au niveau du client de la console distante. Pour plus d'informations, reportez-vous à la section « Touches d'activation de la console distante » (Touches d'activation de la console distante à la page 93).

- Configuration de la correspondance entre les caractères

  En général, avec le jeu de caractères ASCII, les caractères de contrôle (code ASCII inférieur à 32) ne sont pas imprimables et ne peuvent pas être affichés. Ces caractères peuvent servir à représenter des flèches, des étoiles ou des ronds. Certains d'entre eux sont associés à des représentations ASCII. Les équivalents suivants sont ainsi pris en charge :

Valeur du caractère	Description	Équivalent associé
0x07	Beep	*
0x0F	Soleil	*
0x10	Pointeur vers la droite	>
0x11	Pointeur vers la gauche	<
0x18	Flèche vers le haut	^
0x19	Flèche vers le bas	v
0x1A	Flèche gauche	>
0x1B	Flèche droite	>
0x1E	Pointeur vers le haut	^
0x1F	Pointeur vers le bas	v
0xFF	Case ombrée	espace

Utilisation d'une session Linux

Il est possible d'exécuter un port série virtuel iLO 2 sur un système Linux, si ce système est configuré de manière à pouvoir utiliser une session de terminal sur le port série. Cette fonction vous permet d'utiliser un service de consignation à distance. Vous avez ainsi la possibilité de vous connecter à

distance au port série et de rediriger les données générées vers un fichier journal. Tous les messages système à destination du port série sont ainsi consignés à distance.

```
Virtual Serial Port active: IO=0x0408 INT=4

Red Hat Linux release 7.2 (Enigma)
Kernel 2.4.7-10 on an i686

localhost.localdomain login: root
Password:
Last login: Fri Oct  1 17:11:08 on tty1
You have new mail.
[root@localhost root]# tail -f /var/log/messages
Oct  1 16:59:50 localhost  -- root[1014]: ROOT LOGIN ON tty1
Oct  1 17:08:54 localhost login(pam_unix)[1014]: session closed for user root
Oct  1 17:11:06 localhost /sbin/mingetty[1947]: tty1: invalid character ^[ in lo
gin name
Oct  1 17:11:08 localhost login(pam_unix)[1951]: session opened for user root by
 LOGIN(uid=0)
Oct  1 17:11:08 localhost  -- root[1951]: ROOT LOGIN ON tty1
Oct  1 17:11:34 localhost login(pam_unix)[1951]: session closed for user root
Oct  1 17:15:52 localhost login(pam_unix)[1020]: session closed for user root
Oct  1 17:27:50 localhost login(pam_unix)[2004]: session opened for user root by
 LOGIN(uid=0)
Oct  1 17:27:50 localhost  -- root[2004]: DIALUP AT ttyS0 BY root
Oct  1 17:27:50 localhost  -- root[2004]: ROOT LOGIN ON ttyS0
_
Secure Shell | VT100 | Zmodem | ZDC0410.LOG | 00:01:21 | 80x25 | 18:26:27 | 10/01/04
```

Certains modes texte Linux sont en fait des modes graphiques et ne peuvent pas être affichés au moyen de la console texte iLO 2. C'est le cas, par exemple, des terminaux SLES. Même s'ils ressemblent à des terminaux texte, ils sont en fait basés sur un mode texte sur graphique et ne peuvent donc pas s'afficher correctement dans la console texte iLO 2. Lorsque vous essayez d'utiliser un mode non pris en charge, la console texte iLO 2 affiche un message indiquant que le serveur fait appel à un mode graphique.

Certaines séquences de caractères au clavier exigées par Linux dans le mode texte risquent de ne pas être transmises à la console texte iLO 2. Ainsi, la combinaison de touches Alt + Tab risque d'être interceptée par le client. La solution consiste à associer une touche d'activation à cette combinaison. Pour plus d'informations, reportez-vous à la section « Touches d'activation de la console distante » (Touches d'activation de la console distante à la page 93).

Port série virtuel et console série distante

Le processeur de supervision dispose d'un port série pouvant remplacer celui de la carte mère du serveur. À l'aide d'un commutateur électronique, le microprogramme iLO 2 débranche le port série physique du serveur et branche le sien. Ce dernier établit une connexion entre le réseau du processeur de supervision et le serveur. Le microprogramme assemble en paquets les caractères envoyés par le serveur sur le port série et les envoie à l'application ou à l'applet de la console série distante (l'application peut être un client Telnet ou SSH). Les caractères envoyés par l'application ou l'applet distante sont répartis en paquets et envoyés au microprogramme iLO 2. Ce dernier extrait les caractères et les envoie au serveur. La console série distante iLO 2 offre une communication série bidirectionnelle entre l'utilisateur distant et le serveur.

À l'aide de la console série distante iLO 2, l'utilisateur distant peut effectuer les actions suivantes : interagir avec la séquence POST du serveur et la séquence boot du système d'exploitation, établir une session de connexion avec le système d'exploitation, interagir avec ce dernier, exécuter et interagir avec les applications sur le système d'exploitation du serveur. Les utilisateurs de Microsoft® Windows Server™ 2003 peuvent exécuter le sous-système EMS via la console série distante. EMS est utile pour résoudre les problèmes au niveau du démarrage et du noyau du système d'exploitation.

Remote Serial Console (Console série distante)

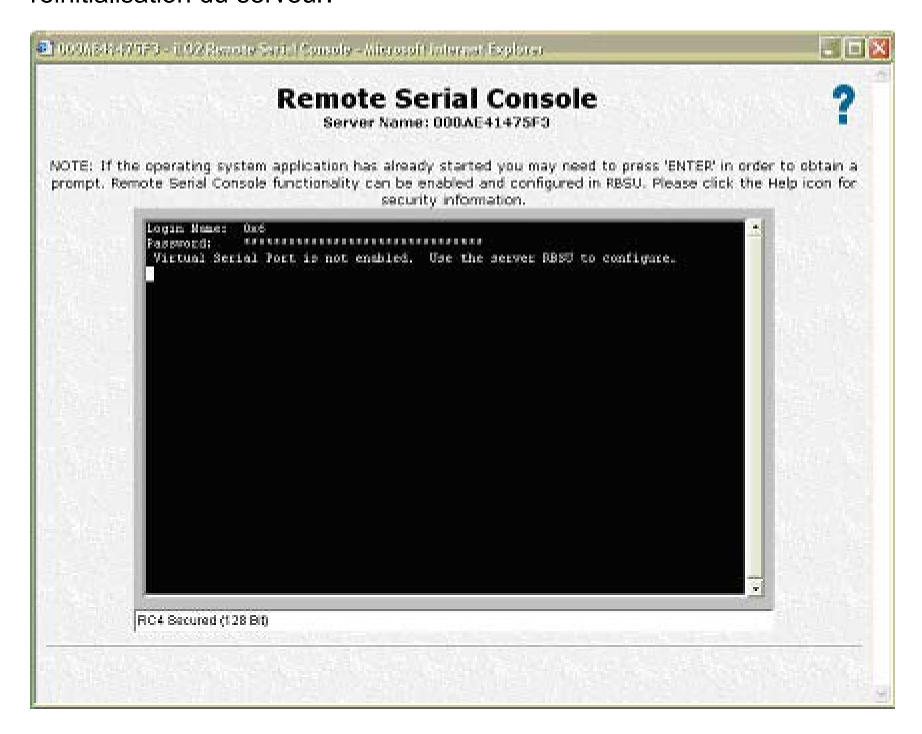
L'option Remote Serial Console (Console série distante) vous permet d'accéder à une console série VT320 à partir d'une console basée sur une applet Java™ connectée au Virtual Serial Port (Port série

virtuel) de iLO 2 à l'aide d'un navigateur. L'activation de la fonction Remote Serial Console (Console série distante) vous permet d'échanger des données textuelles avec l'hôte. Cette option est compatible avec les deux systèmes d'exploitation hôtes Windows® et Linux et requiert JVM.

Les données suivent un flux bidirectionnel envoyé au port série du serveur. Trois types de données peuvent apparaître sur un port série de serveur HP ProLiant :

- Console Windows® EMS
- Session utilisateur Linux via tty série (ttyS0)
- Boîte de dialogue System POST (Test POST du système), si la redirection de la console série BIOS est activée

Lorsque vous cliquez sur l'onglet Remote Console (Console distante), la configuration actuelle s'affiche dans la page Remote Console Information (Informations sur la console distante). Vous pouvez modifier les paramètres en cours en utilisant l'utilitaire RBSU du système hôte, accessible au moment d'une réinitialisation du serveur.



Configuration de la console série distante

Pour utiliser la console série distante avec succès, le logiciel et le microprogramme du serveur doivent être correctement configurés. Pour configurer le microprogramme POST du serveur, l'utilitaire RBSU système du serveur doit valider les paramètres du port série. Vous devez configurer le RBSU pour activer le mode BIOS Serial Console Redirection (Redirection de la console série BIOS). Ce mode demande à la ROM système du serveur d'envoyer/de recevoir des données vers et en provenance du port série du serveur. Lorsque le microprogramme iLO 2 accède au mode Remote Serial Console (Console série distante), iLO 2 active un port série à la place du port série du serveur, intercepte et retransmet les données sortantes vers le client de la console série distante, reçoit les données entrantes (en provenance du client de la console série distante) et les retransmet à la ROM système.

Lorsque le serveur a terminé le test POST, la ROM système du serveur passe le contrôle au chargeur boot du système d'exploitation. Si vous utilisez Linux, vous pouvez configurer le chargeur boot du système d'exploitation pour interagir avec le port série du serveur à la place du clavier, de la souris et de la console VGA. Ceci vous permet d'afficher et d'interagir avec la séquence boot du système

d'exploitation via la console série distante. Pour accéder à un exemple de chargeur boot de système d'exploitation Linux, reportez-vous à la section « Exemple de configuration Linux » (Exemple de configuration Linux à la page 114).

Lorsque le chargeur boot du système d'exploitation a terminé, le système d'exploitation continue de charger. Si vous utilisez un système d'exploitation Linux, vous pouvez le configurer pour qu'il fournisse une session de connexion au système via le port série, la console série distante vous invitant à entrer l'ID et le mot de passe de connexion de l'utilisateur système. Cette configuration vous permet d'interagir avec le système d'exploitation en tant qu'utilisateur de ce système d'exploitation ou administrateur système.

D'autres étapes de configuration supplémentaires sont requises pour utiliser la console série distante (en comparaison avec l'utilisation de la console distante ou IRC), mais la console série distante permet aux utilisateurs Telnet ou SSH d'interagir avec le serveur à distance et sans nécessiter de licence avancée iLO 2. C'est la seule manière qu'à iLO 2 de présenter une console distante véritable basée sur du texte.

Exemple de configuration Linux

Le chargeur boot est l'application qui charge à partir d'un périphérique amorçable lorsque la ROM système du serveur termine le test POST. Pour le système d'exploitation Linux, le chargeur boot généralement utilisé est GRUB. Pour configurer l'utilisation de la console série distante par GRUB, modifiez le fichier de configuration GRUB pour qu'il ressemble à ce qui suit (exemple de Red Hat Linux 7.2 illustré) :

```
serial -unit=0 -speed=115200
terminal -timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2) /grub/splash.zpm.gz
title Red Hat Linux (2.4.18-4smp)
root (hd0,2)
kernel /vmlinuz-2.4.18-4smp ro root=/dev/sda9 console=tty0
console=ttyS0,115200
initrd /initrd-2.4.18-rsmp.img
```

Lorsque Linux a été complètement amorcé, une console de connexion peut être redirigée vers le port série. Les périphériques /dev/ttyS0 et /dev/ttyS1, s'ils ont été configurés, permettent d'obtenir des sessions tty série via la console série distante. Pour commencer une session shell sur un port série configuré, ajoutez la ligne suivante au fichier /etc/inittab pour lancer automatiquement le processus de connexion lors de l'amorçage du système (cet exemple invoque la console de connexion sur /dev/ttyS0) :

```
Sx:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
```

Pour plus d'informations sur la configuration de Linux utilisée avec la console série distante, reportez-vous au document technique *Integrated Lights-Out Virtual Serial Port configuration and operation HOWTO* (Manuel pratique de configuration et de fonctionnement du port série virtuel Integrated Lights-Out) sur le site Web HP (http://www.hp.com/servers/lights-out).

Améliorations du port série virtuel

Le microprogramme iLO 2, version 1.35 met en œuvre un marqueur dynamique qui informe instantanément la ROM système du serveur d'une connexion de console série distante iLO 2. Lorsque le code POST de la ROM système reconnaît la connexion de la console série distante, le système commence à rediriger l'entrée et la sortie de la console vers le port série du serveur et la console série distante. Vous pouvez établir une session de console série distante à tout moment ou pendant la séquence POST système, et vous pouvez afficher et modifier le code POST. Après avoir fermé la session de console série distante, le microprogramme iLO 2 réinitialise le marqueur dynamique pour

informer la ROM système du serveur que la session n'est plus active. Puis, la ROM système du serveur annule la redirection vers le port série du serveur.

Pour rendre cette amélioration opérationnelle, l'utilitaire RBSU de la ROM système doit être configuré pour utiliser le port série virtuel iLO 2. Pour plus d'informations, reportez-vous à la section « Configuration de la console série distante » (Configuration de la console série distante à la page 113).

Console Windows® EMS

Lorsqu'elle est activée, la console Windows® EMS permet d'exécuter l'EMS (Emergency Management Services) lorsque des fonctions vidéo, des drivers de périphérique ou d'autres fonctionnalités du système d'exploitation empêchent le fonctionnement normal du système et l'exécution d'actions correctives normales.

Cependant, iLO 2 permet d'utiliser EMS sur le réseau à l'aide d'un navigateur Web. La fonction Microsoft® EMS permet d'afficher les processus en cours d'exécution, de modifier leur priorité et de les arrêter. La console EMS et la console distante iLO 2 peuvent être utilisées simultanément.

Le port série Windows® EMS doit être activé via l'utilitaire RBSU du système hôte. La configuration permet d'activer ou de désactiver le port EMS, ainsi que de sélectionner le port COM. Le système iLO 2 détecte automatiquement si le port EMS est activé ou désactivé et le port COM sélectionné.

Pour accéder à l'invite `SAC>`, il peut s'avérer nécessaire de saisir `Enter` après s'être connecté via la console du port série virtuel.

Pour plus d'informations sur l'utilisation des fonctions EMS, reportez-vous à la documentation de Windows® Server 2003.

Mode brut de port série virtuel

Vous pouvez utiliser la fonction de port série virtuel de iLO 2 pour connecter un débogueur de noyau Windows® à partir d'un client distant utilisant WiLODbg.exe. WiLODbg.exe contourne le décodage des octets par le microprogramme iLO 2. Une fois le décodage des octets contourné, le port série virtuel passe en mode RAW (non-traité) et directement envoyé au port série.

L'utilitaire WiLODbg.exe est exécuté sur un système client avec l'application WinDBG.exe ou KD.exe Microsoft® installée. Lorsque vous exécutez WiLODbg.exe, il établit une connexion de port série virtuel vers iLO 2 et active le mode RAW. WiLODbg.exe démarre également automatiquement WinDBG.exe avec les commutateurs appropriés nécessaires pour que WinDBG.exe se connecte au périphérique iLO 2 distant.

Pour configurer le serveur, vous devez configurer le RBSU système :

1. Pour activer un port série virtuel, affectez-le à un port COM à partir du menu System Options (Options système).
2. Définissez BIOS Serial Console Port (Port console série BIOS) et EMS Console (Console EMS) sur **Disable** (Désactiver) ou sur le même port que le port série intégré.
3. Définissez le port de débogage Microsoft® Windows® sur le même port que le port série virtuel. Vous pouvez utiliser la commande `bootcfg` ou modifier le fichier boot.ini.

   Exemple d'utilisation de la commande `bootcfg` :

   À l'invite de commande sur un serveur Windows®, entrez la commande suivante :

   ```
   Bootcfg /debug on /port com2 /baud 115200 /id 1
   ```

   Exemple de fichier boot.ini modifié :

```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Debug (com2)" /
fastdetect /debug /debugport=com2 /baudrate=115200
```

Si le serveur est configuré en mode de débogage et qu'une connexion de port série virtuel normale est établie au démarrage du serveur, plusieurs octets de données de débogage sont envoyés au client du port série virtuel. Pour éviter ceci, ne démarrez pas le serveur en mode de débogage lorsqu'une connexion de port série virtuel normale est utilisée.

La configuration du port série affiche les informations de configuration du serveur, les ports série disponibles et l'état du port série virtuel. L'état apparaît comme suit :

- Available (Disponible) - Le port série virtuel n'est pas utilisé
- In use (En cours d'utilisation) - Mode normal lorsque le port série virtuel est connecté normalement
- In use (En cours d'utilisation) - Mode brut lorsque l'utilitaire WiLODbg.exe est utilisé pour la connexion

Lorsque le port série virtuel est utilisé, le bouton Disconnect (Déconnecter) est activé et peut être utilisé pour mettre fin à tout type de connexion de port série virtuel. L'utilisation des fonctions Disconnect (Déconnecter) pour mettre fin à une connexion de port série virtuel établie à l'aide de SSH déconnecte complètement la connexion SSH et ne revient pas à l'invite `</>hpiLO->`. Une déconnexion similaire se produit si la connexion de port série virtuel est établie à l'aide de telnet. Si une applet de connexion série distante est utilisée pour réaliser la connexion à partir d'un navigateur, l'applet est déconnectée. La fenêtre de l'applet doit être fermée et rouverte pour rétablir la connexion série distante.

Utilisation d'un débogueur de noyau Windows distant

Pour démarrer un débogueur de noyau Windows®, vous devez lancer l'utilitaire WiLODbg.exe sur un système client doté de Microsoft® WinDBG.exe ou KD.exe installé, puis redémarrer le serveur distant en mode de débogage pour relier le débogueur. WiLODbg démarre automatiquement WinDBG.exe ou KD.exe. Par exemple :

```
WiLODbg <IP Address>[ -c CommandLine][ -e][ -k][ -p Password][ -s
SocketNumber][
-t][ -u Username]
If a parameter has whitespace in it, enclose it in quotes.
```

Paramètres obligatoires :

`Adresse IP = <Chaîne>` : adresse IP sous forme de chiffres séparés par un point ou nom UNC complet. <Chaîne> représente une série de caractères. Les paramètres obligatoires doivent apparaître dans l'ordre illustré dans l'exemple.

Paramètres facultatifs :

- `-c Ligne_commande = <Chaîne>` : envoie des paramètres de ligne de commande supplémentaires au débogueur sélectionné. Si des espaces ou des tirets (-) sont présents, entourez-les de guillemets anglais. <Chaîne> représente une série de caractères.
- `-e = <Booléen>` : active le cryptage de la liaison de communication. Le cryptage fonctionne uniquement avec l'option telnet dans cette version. Il est désactivé par défaut.
- `-k = <Booléen>` : utilise KD au lieu de WinDbg. La valeur par défaut est d'utiliser WinDbg.

- `-p Mot_passe = <Chaîne>` : définit le mot de passe de connexion à iLO 2. Si non fourni, un mot de passe est demandé. `<Chaîne>` représente une série de caractères.
- `-s Numéro_socket = <Entier>` : définit le numéro de socket pour la connexion à iLO 2. Numéro_socket doit correspondre au paramètre du port de données série brutes sur l'iLO 2 auquel vous vous connectez. La socket 3002 est la valeur par défaut. `<Entier> = [signe]chiffres.`
- `-t = <Booléen>` : utilise une connexion telnet de façon indirecte depuis le débogueur via cet utilitaire. La connexion de socket à la socket 3002 est le paramètre par défaut.
- `-u Nom_utilisateur = <Chaîne>` : définit le nom d'utilisateur de connexion à iLO 2. Si non fourni, un nom d'utilisateur est demandé. <Chaîne> représente une série de caractères. Les options peuvent apparaître dans tout ordre.

Exemples de ligne de commande :

- Pour se connecter à iLO 2 à l'adresse 16.100.226.57, valider l'utilisateur avec le nom d'utilisateur `admin` et le mot de passe `mon_mot_passe`, puis démarrer WinDBG.exe avec la ligne de commande supplémentaire :

  ```
  wilodbg 16.100.226.57 -c "-b" -u admin -p mypass
  ```

  Cet exemple démarre WinDBG.exe avec une ligne de commande supplémentaire `-b` et utilise une connexion de socket directe de WinDBG.exe vers iLO 2 sur le port 3002.
- Pour se connecter à iLO 2 à l'adresse 16.100.226.57, valider l'utilisateur avec le nom d'utilisateur `admin` et le mot de passe `mon_mot_passe`, puis démarrer `kd` avec une ligne de commande supplémentaire `-b:` pour `kd` :

  ```
  wilodbg 16.100.226.57 -k -c "-b" -u admin -p mypass -s 7734
  ```

  Cet exemple démarre `kd` avec une ligne de commande supplémentaire `-b` pour `kd` et utilise une connexion de socket directe de `kd` vers iLO 2 sur le port 7734. Pour pouvoir l'utiliser, vous devez configurer le port 7734 sur iLO 2.
- Pour se connecter à iLO 2 à l'adresse 16.100.226.57 et demander un nom d'utilisateur et un mot de passe :

  ```
  wilodbg 16.100.226.57 -c "-b" -t -e
  ```

  Cet exemple démarre WinDBG.exe avec une ligne de commande supplémentaire `-b`, utilise une connexion telnet cryptée entre WiLODbg et iLO 2 et transmet les données WinDBG.exe via l'utilitaire vers la connexion telnet cryptée.

Support virtuel

Virtual Media (Support virtuel) est une fonction sous licence. Si elle ne fait pas l'objet d'une licence, le message `iLO 2 feature not licensed` (Aucune licence pour la fonction iLO 2) apparaît. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21). La possibilité d'utiliser la fonction Virtual Media (Support virtuel) iLO 2 est accordée ou restreinte via les privilèges utilisateur iLO 2. Vous devez disposer du privilège Virtual Media (Support virtuel) pour sélectionner un périphérique de support virtuel et le connecter au serveur hôte.

L'option iLO 2 Virtual Media permet d'utiliser une unité de disquette virtuelle et une unité de CD/DVD-ROM pour amener un serveur hôte distant à s'initialiser et à utiliser un support standard à partir de tout emplacement du réseau. Les lecteurs Virtual Media (Support virtuel) sont disponibles lorsque le système hôte démarre. Les lecteurs de support virtuel iLO 2 se connectent au serveur hôte à l'aide de la technologie USB. USB apporte de nouvelles fonctionnalités aux périphériques de support virtuel iLO 2

lorsqu'ils sont connectés à des systèmes d'exploitation qui prennent en charge USB. Les différents systèmes d'exploitation offrent des niveaux de prise en charge USB variables.

- Si la fonctionnalité Virtual Floppy (Disquette virtuelle) est activée, l'unité de disquette sera inaccessible depuis le système d'exploitation client.
- Si la fonctionnalité Virtual CD/DVD-ROM est activée, l'unité de CD/DVD-ROM sera inaccessible à partir du système d'exploitation client.

△ **ATTENTION :** Afin d'éviter que les fichiers et les données ne soient corrompus, n'accédez pas au support local lorsque celui-ci est utilisé comme support virtuel.

Vous pouvez accéder à un support virtuel sur un serveur hôte à partir d'un client via une interface graphique à l'aide d'une applet Java™ et via une interface de scripts à l'aide d'un moteur XML. Aucun délai d'attente n'est associé à l'applet Virtual Media lorsqu'elle est connectée au serveur hôte. Elle se ferme si l'utilisateur se déconnecte.

Pour accéder aux périphériques iLO 2 Virtual Media depuis une interface basée sur un navigateur, cliquez sur **Virtual Media>Virtual Media Applet** (Support virtuel>Applet de support virtuel). Une applet est chargée afin de prendre en charge le périphérique de disquette virtuelle ou de CD/DVD-ROM virtuelle.

Vous pouvez également accéder à l'option Virtual Media (Support virtuel) via l'option Integrated Remote Console (Console distante intégrée). L'option Integrated Remote Console (Console distante intégrée) permet d'accéder au système KVM et de contrôler les fonctions Virtual Power (Alimentation virtuelle) et Virtual Media (Support virtuel) à partir d'une seule et unique console dans Microsoft® Internet Explorer. Pour plus d'informations sur l'accès aux fonctions Virtual Power (Alimentation virtuelle) et Virtual Media (Support virtuel) à l'aide de la console distante intégrée, reportez-vous à la section « Option Integrated Remote Console (Console distante intégrée) » (Option Integrated Remote Console (Console distante intégrée) à la page 96).

Utilisation des périphériques de support virtuel iLO 2

Vous pouvez accéder à un support virtuel sur un serveur hôte à partir d'un client via une interface graphique à l'aide d'une applet Java™ et via une interface de scripts à l'aide d'un moteur XML.

Pour accéder aux périphériques de support virtuel iLO 2 depuis l'interface graphique, sélectionnez l'option **Virtual Media** (Support virtuel) sous l'onglet Virtual Devices (Périphériques virtuels). Une applet est chargée afin de prendre en charge le périphérique de disquette virtuelle ou de CD/DVD-ROM virtuelle.

Virtual Media et Windows 7

Par défaut, Windows 7 interrompt l'alimentation du concentrateur virtuel iLO en l'absence de périphériques de support virtuel activés ou connecté au démarrage. Pour empêcher ce problème, remplacez manuellement la fonction de supervision de l'alimentation dans Windows 7 au travers du Panneau de configuration afin que le concentrateur virtuel ne perde pas son alimentation.

1. Ouvrez le **Gestionnaire de périphériques**.
2. Cliquez sur **Affichage**.
3. Sélectionnez **Périphériques par connexion** dans le menu.
4. Sélectionnez et développez **Contrôleur hôte PCI vers USB standard universel** pour afficher les périphériques USB, y compris le concentrateur USB générique. L'option Concentrateur USB générique est le contrôleur du concentrateur USB virtuel d'iLO 2.
5. Cliquez avec le bouton droit sur **Concentrateur USB générique** et sélectionnez **Propriétés**.

6. Sélectionnez l'onglet **Gestion de l'alimentation**.

7. Désactivez la case **Autoriser l'ordinateur à éteindre ce périphérique pour économiser l'énergie**.

Lecteur de disquette/clé USB virtuel iLO 2

L'unité de disquette virtuelle iLO 2 est disponible pour tous les systèmes d'exploitation au moment de l'initialisation du système. L'initialisation depuis la disquette virtuelle iLO 2 permet notamment de mettre à niveau la mémoire ROM du système hôte, d'installer un système d'exploitation depuis des unités en réseau ou d'effectuer une récupération après un incident survenu sur un système d'exploitation.

Si le système d'exploitation du serveur hôte prend en charge les périphériques de mémoire de masse USB ou les périphériques numériques sécurisés, le lecteur de disquette/clé USB virtuel iLO est alors également disponible après le chargement du système d'exploitation du serveur hôte. Le lecteur de disquette/clé USB virtuel iLO 2 peut notamment vous servir lorsque le système d'exploitation du serveur hôte exécute une mise à niveau des drivers de périphérique, crée une disquette de réparation d'urgence et exécute d'autres tâches. Le fait de disposer d'une disquette virtuelle lorsque le serveur est en cours d'utilisation peut s'avérer particulièrement utile si vous devez diagnostiquer et résoudre un problème au niveau du driver de la carte réseau.

Le périphérique de disquette/clé USB virtuelle peut être l'unité de disquette, le lecteur de clé USB ou le lecteur numérique sécurisé physique sur lequel vous exécutez le navigateur Web, ou un fichier image sur votre disque dur local ou sur une unité réseau. Pour des performances optimales, HP vous recommande d'utiliser des fichiers image locaux stockés sur le disque dur de votre PC client, ou sur une unité réseau accessible via une liaison haut débit.

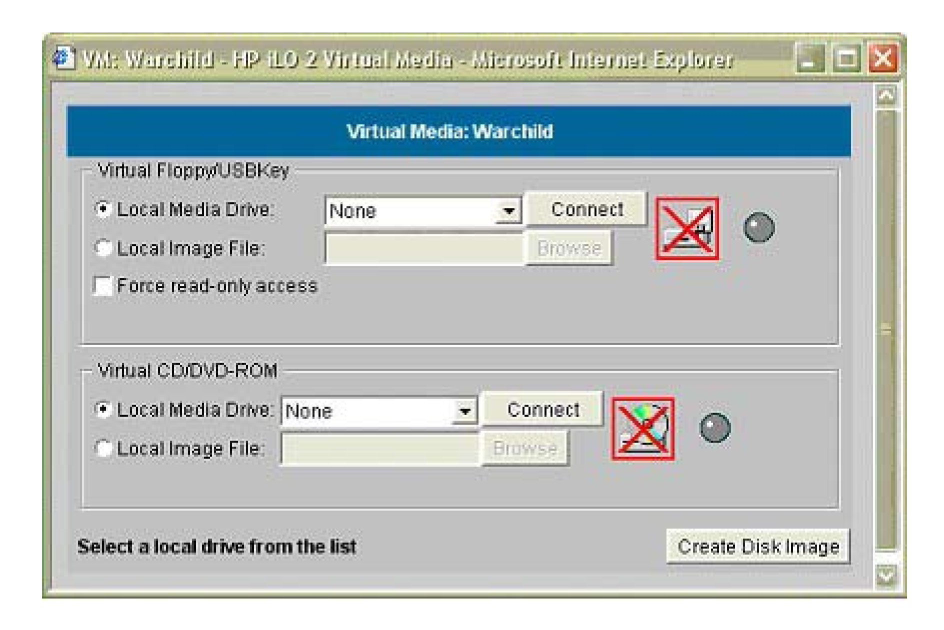
Pour utiliser une unité de disquette ou un lecteur de clé USB physique dans votre ordinateur client, procédez comme suit :

1. Sélectionnez **Local Media Drive** (Unité de support locale) dans la section Virtual Floppy/USBKey (Disquette/Clé USB virtuelle).

2. Dans le menu déroulant, sélectionnez la lettre correspondant à l'unité locale de disquette ou de clé USB physique souhaitée de votre PC client. Pour empêcher que la disquette ou le fichier image source ne soit modifié(e) en cours d'utilisation, sélectionnez l'option **Force read-only access** (Forcer l'accès en lecture seule).

3. Cliquez sur **Connect** (Connecter).

L'icône et le voyant du lecteur connecté changent pour refléter l'état en cours de l'unité de disquette virtuelle.



Pour utiliser un fichier image :

1. Sélectionnez **Local Image File** (Fichier image local) dans la section Virtual Floppy/USB Key (Disquette/Clé USB virtuelle) de l'applet Virtual Media (Support virtuel).
2. Saisissez le chemin ou le nom de fichier de l'image dans la zone de texte, ou cliquez sur **Browse** (Parcourir) pour trouver le fichier image à l'aide de la boîte de dialogue Choose Disk Image File (Choisir le fichier d'image disque). Pour empêcher que la disquette ou le fichier image source ne soit modifié(e) en cours d'utilisation, sélectionnez l'option **Force read-only access** (Forcer l'accès en lecture seule).
3. Cliquez sur **Connect** (Connecter).

L'icône et le voyant du lecteur connecté changent pour refléter l'état en cours de l'unité de disquette virtuelle, du lecteur de clé USB ou du périphérique numérique sécurisé. Une fois les périphériques connectés, le serveur hôte peut y accéder jusqu'à ce que vous fermiez l'applet Virtual Media. Lorsque vous avez terminé, vous pouvez soit déconnecter le périphérique du serveur hôte, soit fermer l'applet.

REMARQUE : l'applet Virtual Media doit rester ouverte dans votre navigateur tant que vous continuez d'utiliser un périphérique de support virtuel.

La disquette/clé USB virtuelle iLO 2 est mise à la disposition du serveur hôte au moment de l'exécution si le système d'exploitation de celui-ci prend en charge les unités de disquette ou de clé USB. Reportez-vous à la section « Prise en charge USB par les systèmes d'exploitation (Prise en charge USB par les systèmes d'exploitation à la page 121) » pour plus d'informations sur les systèmes d'exploitation qui prennent actuellement en charge le stockage de masse USB.

La disquette/clé USB virtuelle iLO 2 est reconnue par votre système d'exploitation au même titre que n'importe quelle autre unité. Lorsque vous utilisez iLO 2 pour la première fois, le système d'exploitation hôte peut vous demander d'exécuter un Assistant New Hardware Found (Nouveau matériel détecté).

Lorsque vous avez fini d'utiliser le support virtuel iLO 2 et que vous le déconnectez, le système d'exploitation peut vous envoyer un message d'avertissement indiquant le retrait non sécurisé d'un périphérique. Cet avertissement peut être évité à l'aide de la fonction fournie par le système d'exploitation, qui permet d'arrêter le périphérique avant de le déconnecter du support virtuel.

Remarques concernant les systèmes d'exploitation de disquette/clé USB virtuelle

- MS-DOS

  Au cours du démarrage et de sessions MS-DOS, le périphérique de disquette virtuelle apparaît sous forme d'unité de disquette BIOS standard. Ce périphérique apparaît en tant qu'unité A. Si une unité de disquette reliée physiquement existe, elle est obscurcie et indisponible durant cette période. Vous ne pouvez pas utiliser simultanément une unité de disquette physique locale et la fonction Virtual Floppy (Disquette virtuelle).

- Windows Server® 2008 ou version ultérieure et Windows Server® 2003

  Les lecteurs de disquette et de clé USB virtuels s'affichent automatiquement dès que Microsoft® Windows® a reconnu le montage du périphérique USB. Utilisez-les comme vous le feriez d'un périphérique connecté localement.

  Pour utiliser la fonctionnalité Virtual Floppy (Disquette virtuelle) pour recourir à une disquette de drivers lors d'une installation Windows®, désactivez l'unité de disquette intégrée à l'hôte RBSU, car c'est lui qui oblige la disquette virtuelle à apparaître sous la lettre d'unité A.

  Pour utiliser la fonctionnalité Virtual USB Key (Clé USB virtuelle) pour recourir à une disquette de drivers lors d'une installation Windows®, modifiez l'ordre d'initialisation du lecteur de clé USB dans l'utilitaire RBSU du système. HP recommande de placer le lecteur de clé USB en premier dans l'ordre d'initialisation.

- Windows Vista®

  La fonction Virtual Media (Support virtuel) ne fonctionne pas correctement sous Windows Vista™ lorsqu'Internet Explorer 7 est utilisé avec le mode protégé activé. Si vous tentez d'utiliser un support virtuel avec le mode protégé activé, divers messages d'erreur s'affichent, notamment `could not open cdrom (the parameter is incorrect)` (Impossible d'ouvrir le CD-ROM. Paramètre incorrect). Pour utiliser le support virtuel, cliquez sur **Outils/Options Internet/Sécurité**, désactivez l'option **Activer le mode protégé**, puis cliquez sur **Appliquer**. Une fois le mode protégé désactivé, vous devez fermer toutes les instances du navigateur ouvertes, puis redémarrer le navigateur.

- NetWare 6.5

  NetWare 6.5 prend en charge l'utilisation d'unités de disquette et de clé USB. Reportez-vous à la section « Montage d'une disquette/clé virtuelle USB sous NetWare 6.5 (Montage d'une disquette/clé virtuelle USB sous NetWare 6.5 à la page 122) » pour obtenir des instructions détaillées.

- Red Hat et SUSE Linux

  Linux prend en charge l'utilisation d'unités de disquette et de clé USB. Reportez-vous à la section « Montage d'un support/clé virtuel USB sous Linux (Montage d'un support/clé virtuel USB sous Linux à la page 122) » pour obtenir des instructions détaillées.

Prise en charge USB par les systèmes d'exploitation

Pour pouvoir utiliser les lecteurs du support virtuel, votre système d'exploitation doit prendre en charge les périphériques USB. Il doit également prendre en charge les périphériques de mémoire de masse USB. À l'heure actuelle, les systèmes d'exploitation prenant en charge les périphériques USB sont les suivants : Windows Server® 2008, Windows® 2003, Red Hat Enterprise Linux 3, Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, SUSE SLES 9 et SUSE SLES 10. Il se peut que d'autres systèmes d'exploitation prennent également en charge les périphériques de mémoire de masse USB.

Au démarrage du système, le BIOS de la mémoire BIOS offre un support USB jusqu'à ce que le système d'exploitation soit chargé. Étant donné que MS-DOS utilise le BIOS pour communiquer avec les périphériques de stockage, les disquettes d'utilitaires permettant de lancer DOS fonctionneront également avec le support virtuel.

REMARQUE : sous RedHat Enterprise Linux 3, vous ne pouvez pas utiliser de disquette de driver à l'aide du support virtuel.

Montage d'une disquette/clé virtuelle USB sous NetWare 6.5

1. Accédez à la carte iLO 2 à l'aide d'un navigateur.
2. Sélectionnez **Virtual Media** (Support virtuel) sous l'onglet Virtual Devices (Périphériques virtuels).
3. Introduisez le support dans l'unité de disquette locale, sélectionnez une unité de disquette, puis cliquez sur **Connect** (Connecter). Vous pouvez également sélectionner une image de disquette, puis cliquer sur **Connect** (Connecter).

Sous NetWare 6.5, entrez la commande `lfvmount` sur la console du serveur pour affecter au périphérique une lettre correspondant à l'unité.

Le système d'exploitation NetWare 6.5 choisit la première lettre disponible pour l'unité de disquette virtuelle. Les commandes `volumes` peuvent alors être utilisées par la console du serveur pour afficher l'état de montage de cette nouvelle unité.

Lorsque la lettre choisie pour représenter la nouvelle unité s'affiche indiquant que cette dernière est à présent montée, l'unité est alors accessible via l'interface graphique du serveur et la console système.

Lorsque l'unité de disquette virtuelle est montée, si le support est changé dans l'unité de disquette locale, la commande `lfvmount` devra être une nouvelle fois émise à partir de la console du serveur afin que le nouveau support soit visible dans le système d'exploitation NetWare 6.5.

Montage d'un support/clé virtuel USB sous Linux

1. Accédez à la carte iLO 2 à l'aide d'un navigateur.
2. Sélectionnez **Virtual Media** (Support virtuel) sous l'onglet Virtual Devices (Périphériques virtuels).
3. Sélectionnez un lecteur ou une image de disquette.
   a. Pour un lecteur ou une image de disquette, sélectionnez Local Media Drive (Unité de support locale) ou Local Image File (Fichier image local) et cliquez sur **Connect** (Connecter).
   b. Pour un lecteur ou une image de clé USB, sélectionnez Local Image File (Fichier image local) et cliquez sur **Connect** (Connecter).

      Pour un lecteur de clé USB physique, saisissez `/dev/sda` dans la zone de texte Local Image File (Fichier image local).
4. Chargez les drivers USB à l'aide des commandes suivantes :

```
modprobe usbcore
modprobe usb-storage
modprobe usb-ohci
```

5. Chargez le driver de disquettes SCSI à l'aide de la commande suivante :

```
modprobe sd_mod
```

6. Montez le lecteur.
   - Pour monter le lecteur de disquette, utilisez la commande suivante :

     ```
     mount /dev/sda /mnt/floppy -t vfat
     ```
   - Pour monter le lecteur de clé USB, utilisez la commande suivante :

     ```
     mount /dev/sda1 /mnt/keydrive
     ```

REMARQUE : utilisez la commande `man mount` pour d'autres types de systèmes de fichiers.

L'unité de disquette et de clé peut être utilisée comme un système de fichiers Linux, si elle est formatée comme telle à l'aide de la commande `mount`. Cependant, les disquettes de 1,44 Mo de capacité sont en général accessibles à l'aide des utilitaires mtools fournis avec Red Hat et SLES. La configuration des utilitaires mtools par défaut ne reconnaît pas une disquette connectée via l'USB. Pour activer les différentes commandes m permettant d'accéder au périphérique Virtual Floppy (Disquette virtuelle), modifiez le fichier /etc/mtools.conf existant et ajoutez la ligne suivante :

```
drive v: file="/dev/sda" exclusive
```

Pour activer les différentes commandes mtools permettant d'accéder au lecteur de clé USB virtuel, modifiez le fichier /etc/mtools.conf existant et ajoutez la ligne suivante :

```
drive v: file="/dev/sda1" exclusive
```

Pour afficher la table des partitions du lecteur de clé USB virtuel afin de rechercher la partition souhaitée, utilisez la commande suivante :

```
fdisk -l /dev/sda
```

Cette modification permet au progiciel mtools d'accéder au périphérique Virtual Floppy (Disquette virtuelle) en le désignant à l'aide de la lettre v. Par exemple :

```
mcopy /tmp/XXX.dat v:
mdir v:
mcopy v:foo.dat /tmp/XXX
```

Changement de disquette

Lorsque vous utilisez l'unité de disquette ou de clé USB virtuelle iLO 2 et que l'unité de disquette physique du client est une unité de disquette USB, les changements de disquette ne sont pas reconnus. Par exemple, dans cette configuration, si une liste des répertoires provient d'une disquette et que vous changez cette dernière, les listes de répertoires ultérieures correspondront à celle de la première disquette utilisée. Si des changements de disque sont nécessaires lors de l'utilisation d'une disquette ou clé USB virtuelle iLO 2, assurez-vous que la machine client contient une unité de disquette non-USB.

CD/DVD-ROM virtuel iLO 2

Le CD/DVD-ROM virtuel iLO 2 est accessible, lors de l'amorçage du serveur, par les systèmes d'exploitation mentionnés dans la section « Prise en charge USB par les systèmes d'exploitation » (Prise en charge USB par les systèmes d'exploitation à la page 121). L'initialisation depuis le CD/DVD-ROM virtuel iLO 2 permet notamment de déployer un système d'exploitation depuis des unités réseau et d'effectuer une récupération après un incident survenu sur un système d'exploitation.

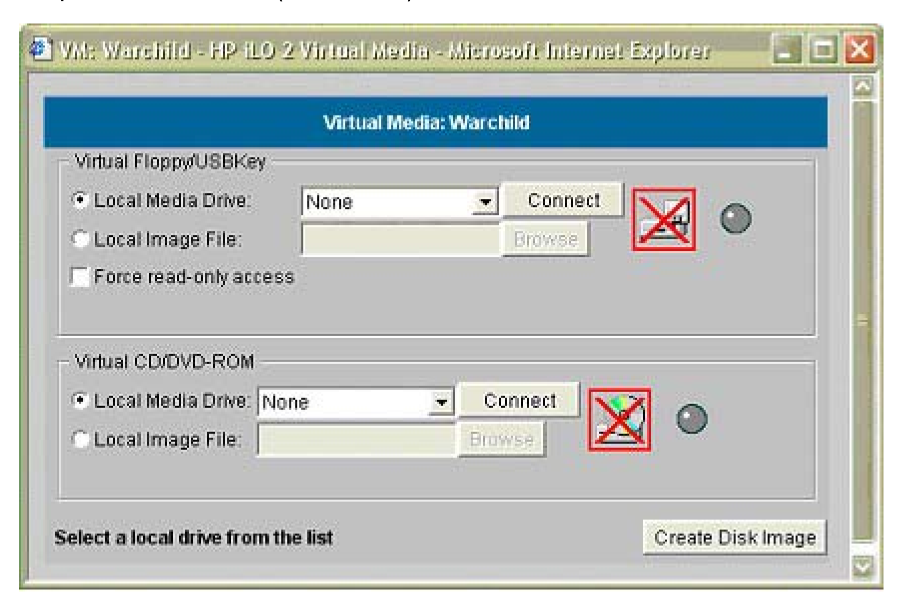
Si le système d'exploitation du serveur hôte prend en charge les périphériques de mémoire de masse USB, le CD/DVD-ROM virtuel iLO 2 est alors également disponible après le chargement du système d'exploitation du serveur hôte. Le CD/DVD-ROM virtuel iLO 2 peut vous servir lorsque le système d'exploitation du serveur hôte exécute une mise à niveau des drivers de périphérique, installe des logiciels ou réalise d'autres tâches. Le fait de disposer d'un CD/DVD-ROM virtuel lorsque le serveur est en cours d'utilisation peut s'avérer particulièrement utile si vous devez diagnostiquer et résoudre un problème au niveau du driver de la carte réseau.

Le CD/DVD-ROM virtuel peut être l'unité de CD/DVD-ROM physique sur laquelle vous exécutez le navigateur Web ou un fichier image sur votre disque dur local ou sur une unité réseau.

REMARQUE : pour de meilleures performances, utilisez des fichiers image. HP vous recommande d'utiliser des fichiers image locaux stockés sur le disque dur de votre PC client, ou sur une unité réseau accessible via une liaison haut débit.

Pour utiliser une unité de CD/DVD-ROM dans votre PC client :

1. Sélectionnez **Local Media Drive** (Unité de support locale) dans la section Virtual CD/DVD-ROM.
2. Dans le menu déroulant, sélectionnez la lettre correspondant à l'unité de CD/DVD-ROM physique souhaitée de votre PC client.
3. Cliquez sur **Connect** (Connecter).



Pour utiliser un fichier image :

1. Sélectionnez **Local Image File** (Fichier image local) dans la section Virtual CD/DVD-ROM (CD-ROM virtuel) de l'applet Virtual Media.
2. Saisissez le chemin ou le nom de fichier de l'image dans la zone de texte, ou cliquez sur **Browse** (Parcourir) pour trouver le fichier image à l'aide de la boîte de dialogue Choose Disk Image File (Choisir le fichier d'image disque).
3. Cliquez sur **Connect** (Connecter).

L'icône et le voyant de l'unité connectée changent pour refléter l'état en cours de l'unité de CD/DVD-ROM virtuel. Une fois les périphériques virtuels connectés, le serveur hôte peut y accéder jusqu'à ce que vous fermiez l'applet Virtual Media. Lorsque vous avez fini d'utiliser le CD/DVD-ROM virtuel, vous pouvez déconnecter le périphérique du serveur hôte ou fermer l'applet. L'applet Virtual Media doit rester ouverte lorsque vous utilisez un périphérique de support virtuel.

Le CD/DVD-ROM de support virtuel iLO 2 est mis à la disposition du serveur hôte au moment de l'exécution si le système d'exploitation de celui-ci prend en charge les unités de disquette USB. Reportez-vous à la section « Prise en charge USB par les systèmes d'exploitation (Prise en charge USB par les systèmes d'exploitation à la page 121 » pour plus d'informations sur les systèmes d'exploitation qui prennent actuellement en charge le stockage de masse USB.

Le CD/DVD-ROM de support virtuel iLO 2 est reconnu par votre système d'exploitation au même titre que tout autre CD/DVD-ROM. Lorsque vous utilisez iLO 2 pour la première fois, le système d'exploitation hôte peut vous demander d'exécuter un Assistant New Hardware Found (Nouveau matériel détecté).

Lorsque vous avez fini d'utiliser le support virtuel iLO 2 et que vous le déconnectez, le système d'exploitation peut vous envoyer un message d'avertissement indiquant le retrait non sécurisé d'un périphérique. Cet avertissement peut être évité à l'aide de la fonction fournie par le système d'exploitation, qui permet d'arrêter le périphérique avant de le déconnecter du support virtuel.

Remarques sur les systèmes d'exploitation exécutant des CD/DVD-ROM virtuels

- MS-DOS

  Le CD/DVD-ROM virtuel n'est pas pris en charge sous MS-DOS.

- Windows Server® 2008 et Windows Server® 2003

  La fonctionnalité de CD/DVD-ROM virtuel s'affiche automatiquement dès que Windows® a reconnu le montage du périphérique USB. Utilisez-la comme vous utiliseriez une unité de CD/DVD-ROM reliée localement.

- Linux
  - Red Hat Linux

    Sur les serveurs équipés d'une unité de CD/DVD-ROM IDE reliée localement, l'unité de CD/DVD-ROM virtuel est accessible via la commande /dev/cdrom1. Cependant, sur les serveurs sans unité de CD/DVD-ROM reliée localement, tels que les systèmes lame BL-class, le CD/DVD-ROM virtuel est le premier CD/DVD-ROM accessible via la commande /dev/cdrom.

    Le CD/DVD-ROM virtuel peut être monté comme une unité de CD/DVD-ROM normale, à l'aide de la commande :

    mount /mnt/cdrom1
  - SLES 9

    Le système d'exploitation SLES 9 place les CD/DVD-ROM connectés via USB dans un emplacement différent. Par conséquent, il est possible de trouver le CD/DVD-ROM virtuel grâce à la commande /dev/scd0, sauf s'il existe déjà un CD/DVD-ROM local relié via USB, auquel cas il faut utiliser pour ce faire la commande /dev/scd1.

    Le CD/DVD-ROM virtuel peut être monté comme une unité de CD/DVD-ROM normale, à l'aide de la commande :

    mount /dev/scd0 /media/cdrom11

    Reportez-vous à la section « Montage d'un CD/DVD-ROM de support virtuel USB sous Linux » (Montage d'un CD/DVD-ROM de support virtuel USB sous Linux à la page 125).

Montage d'un CD/DVD-ROM de support virtuel USB sous Linux

1. Accédez à la carte iLO 2 à l'aide d'un navigateur.
2. Sélectionnez **Virtual Media** (Support virtuel) sous l'onglet Virtual Devices (Périphériques virtuels).
3. Sélectionnez le CD/DVD-ROM à utiliser, puis cliquez sur **Connect** (Connecter).
4. Montez l'unité de CD-ROM à l'aide de la commande suivante :

   ```
   mount /dev/cdrom1 /mnt/cdrom1
   ```

   Pour SLES 9 :

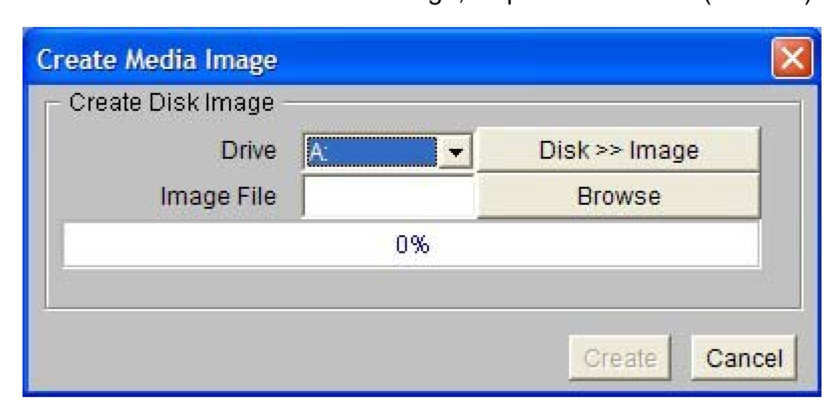
   ```
   mount /dev/scd0 /media/cdrom1
   ```

Création de fichiers d'image disque iLO 2

La fonction Virtual Media (Support virtuel) de iLO 2 permet de créer des fichiers image de disquette et de CD-ROM dans la même applet. La création de fichiers d'image DVD à l'aide de l'applet Virtual Media (Support virtuel) n'est pas prise en charge. Les fichiers image créés à partir de l'applet sont des images du système de fichiers ISO-9660. Le support virtuel iLO 2 est plus performant lorsque des fichiers image sont utilisés. L'utilitaire permettant de créer des fichiers d'image disque de disquette et de CD-ROM iLO 2 est intégré dans l'applet Virtual Media (Support virtuel). Cependant, vous pouvez aussi créer des images à l'aide d'outils standard tels que DD.

Pour créer un fichier image :

1. Cliquez sur **Create Disk Image** (Créer image disque).
2. Sélectionnez l'unité de support locale dans le menu déroulant.
3. Entrez le chemin ou nom de fichier dans la zone de texte ou cliquez sur **Browse** (Parcourir) pour sélectionner un fichier image existant ou pour changer le répertoire dans lequel créer le fichier image.
4. Cliquez sur **Create** (Créer). L'applet Virtual Media (Support virtuel) lance la procédure de création du fichier image. La procédure est terminée lorsque la barre de progression atteint 100 %. Pour annuler la création d'un fichier image, cliquez sur **Cancel** (Annuler).



L'option Disk>>Image (Disque>>Image) permet de créer des fichiers image à partir de disquettes ou de CD-ROM physiques. L'option Image>>Disk (Image>>Disque) n'est pas valide pour une image de CD-ROM virtuel. Le bouton Disk>>Image (Disque>>Image) se transforme en bouton Image>>Disk (Image>>Disque) lorsque vous cliquez dessus. Utilisez ce bouton pour basculer de la création de fichiers image depuis des disquettes physiques à la création de disquettes physiques à partir de fichiers image.

Virtual Folder (Dossier virtuel)

Le dossier virtuel iLO 2 émule un périphérique USB, en créant dynamiquement une image de support d'un dossier ou d'un répertoire sélectionné. Après avoir créé une image virtuelle d'un dossier ou d'un répertoire, le serveur se connecte à l'image créée en tant que périphérique de stockage USB, ce qui permet d'accéder au serveur et de transférer les fichiers de l'image générée par iLO 2 vers n'importe quel emplacement sur le serveur.

La fonction Virtual Folder (Dossier virtuel) est uniquement disponible dans l'IRC. Le dossier virtuel est non amorçable, en lecture seule et le dossier monté est statique. Les modifications apportées au fichier client ne sont pas dupliquées dans le dossier monté.

Virtual Folder (Dossier virtuel) est une fonction sous licence disponible avec l'achat de iLO 2 Advanced ou iLO 2 Select. La fonction Virtual Folder (Dossier virtuel) permet d'accéder, de parcourir et de transférer des fichiers d'un client vers un serveur supervisé. La fonction Virtual Folder prend en charge

la possibilité de monter et démonter un répertoire sur un répertoire local ou en réseau accessible via le client, monté et démonté en tant que périphérique Virtual Media (Support virtuel).

Remarques sur le système d'exploitation du dossier virtuel

- MS-DOS

  Au cours du démarrage et de sessions MS-DOS, le périphérique de dossier virtuel apparaît sous forme d'unité de disquette BIOS standard. Ce périphérique apparaît en tant qu'unité A. Si une unité de disquette reliée physiquement existe, elle est obscurcie et indisponible durant cette période. Vous ne pouvez pas utiliser simultanément une unité de disquette physique locale et la fonction Virtual Folder (Dossier virtuel).

- Windows®

  Le dossier virtuel apparaît automatiquement après que Microsoft® Windows® reconnaît le montage du périphérique USB virtuel. Vous pouvez utiliser le dossier comme n'importe quel périphérique localement relié. Le dossier virtuel n'est pas amorçable. Une tentative d'amorçage depuis le dossier peut empêcher l'amorçage du serveur.

- NetWare 6.5

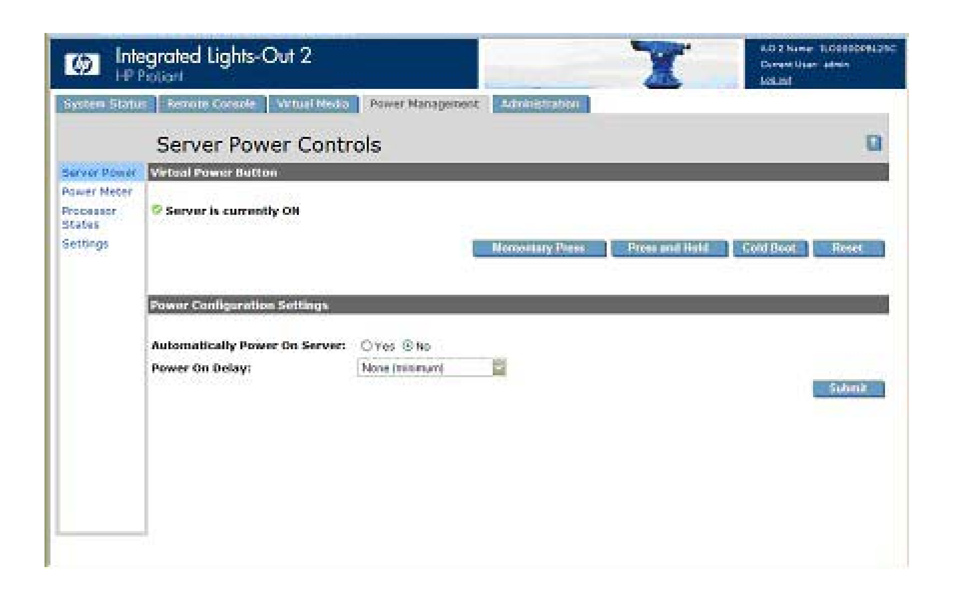
  NetWare 6.5 prend en charge l'utilisation du dossier virtuel en tant qu'unité de disquette et de clé USB. Reportez-vous à la section « Montage d'une disquette/clé virtuelle USB sous NetWare 6.5 » (Montage d'une disquette/clé virtuelle USB sous NetWare 6.5 à la page 122) pour obtenir des instructions détaillées.

- Red Hat et SLES Linux

  Linux prend en charge l'utilisation du dossier virtuel. Le dossier virtuel utilise un format de système de fichiers FAT 16. Pour plus d'informations, reportez-vous à la section « Montage d'un support/clé virtuel USB sous Linux » (Montage d'un support/clé virtuel USB sous Linux à la page 122).

Gestion de l'alimentation

iLO 2 Power Management (Gestion de l'alimentation iLO 2) permet d'afficher et de contrôler l'état de l'alimentation du serveur, de surveiller l'utilisation de l'alimentation, de surveiller le processeur et de modifier les paramètres de l'alimentation. La page Power Management (Gestion de l'alimentation) comporte quatre options de menu : Server Power (Alimentation du serveur), Power Meter (Mesureur de puissance), Processor States (États des processeurs) et Settings (Paramètres). Lorsque vous sélectionnez **Power Management** (Gestion de l'alimentation), la page Server Power Controls (Contrôle de l'alimentation du serveur) s'affiche. La page Server Power Controls (Contrôle de l'alimentation du serveur) se divise en deux sections : Virtual Power Button (Bouton d'alimentation virtuelle) et Power Configuration Settings (Paramètres de configuration de l'alimentation).



La section relative au bouton virtuel d'alimentation présente l'état actuel de l'alimentation du serveur, ainsi que les options de contrôle de l'alimentation du serveur distant. L'état de l'alimentation affiché correspond à l'état de l'alimentation du serveur au moment où la page a été ouverte. Le serveur peut être Activé, Désactivé ou Réinitialisé. Pour actualiser l'indicateur de l'alimentation, utilisez la fonction de rafraîchissement du navigateur.

Pour modifier l'état actuel de l'alimentation du serveur avec les options Virtual Power Button, vous devez disposer des privilèges Virtual Power (Alimentation virtuelle) et Reset (Réinitialisation). Certaines des options de contrôle de l'alimentation ne permettent pas d'arrêter le système d'exploitation de façon progressive et sans perte de données. La fermeture du système d'exploitation doit être initiée à l'aide de la console distante avant d'utiliser les options Virtual Power Button (Bouton d'alimentation virtuelle). Les options suivantes sont disponibles :

- Le bouton Momentary Press (Pression brève) agit de la même façon qu'un bouton d'alimentation physique soumis à une pression brève.
- Press and Hold (Pression prolongée) agit de la même façon qu'un bouton d'alimentation physique qui serait enfoncé pendant cinq secondes, puis relâché. Cette option propose la fonctionnalité compatible ACPI intégrée dans certains systèmes d'exploitation. Ces systèmes d'exploitation se comportent de façon différente suivant la durée de la pression. Le comportement de cette option peut contourner les fonctions d'arrêt sans perte de données du système d'exploitation.
- Cold Boot (Démarrage à froid du système) désactive immédiatement l'alimentation du système. Il redémarre après environ six secondes. Cette option n'est pas disponible lorsque le serveur est éteint. Cette option contourne les fonctions d'arrêt sans pertes de données du système d'exploitation.
- Reset System (Réinitialiser le système) démarre la réinitialisation du système. Cette option n'est pas disponible lorsque le serveur est éteint. Le comportement de cette option peut contourner les fonctions d'arrêt sans perte de données du système d'exploitation.

La section Power Configuration Settings (Paramètres de configuration de l'alimentation) vous permet de contrôler la façon dont le serveur distant se met sous tension à l'aide de l'alimentation. Les options suivantes sont disponibles :

- Automatically Power On Server (Serveur automatiquement sous tension) permet à iLO 2 d'activer un serveur lorsque celui-ci est alimenté, de la même façon que lorsque celui-ci est branché ou lorsque qu'un système d'alimentation sans coupure (UPS) est activé après une panne de courant. Vous devez être doté du privilège Virtual Power and Reset (Alimentation et réinitialisation virtuelles) pour pouvoir modifier ce paramètre.

  Si l'alimentation se coupe de façon imprévue alors que le serveur est sous tension, le serveur se remet automatiquement sous tension, même si le paramètre Serveur automatiquement sous tension est défini sur No (Non).

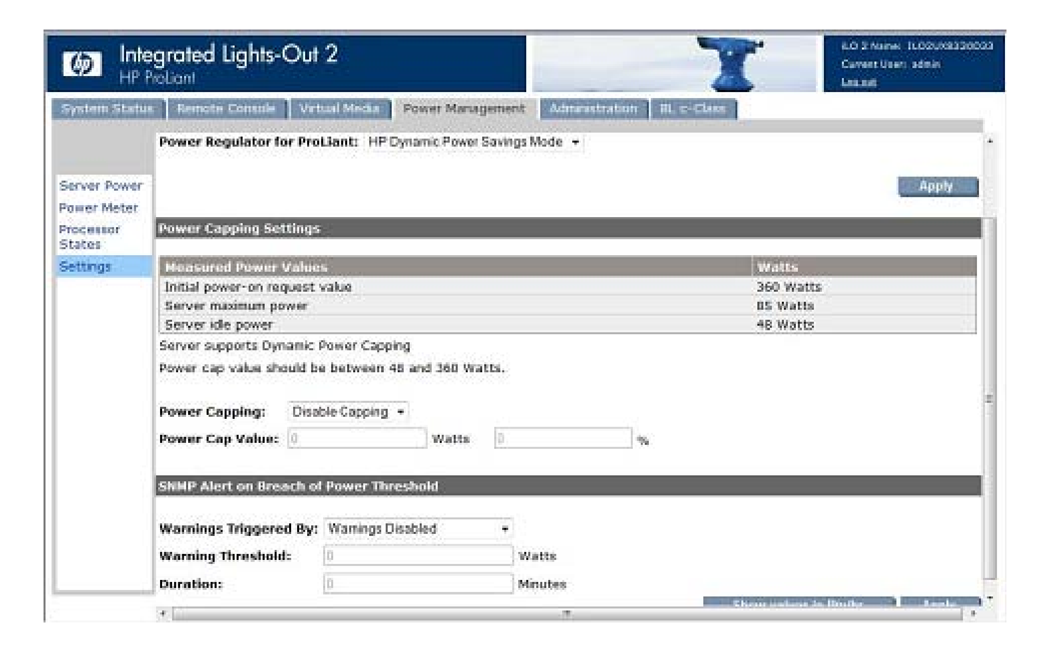
- Power On Delay (Mise sous tension retardée) sert à décaler la mise sous tension d'un serveur dans un centre de données. Les serveurs lame sont régis par l'infrastructure du rack et ne prennent pas en charge une mise sous tension retardée. La mise sous tension retardée ne cause aucune interférence avec le bouton d'alimentation.

  Le délai est établi avant que le serveur ne soit mis sous tension par iLO2 (y compris la mise sous tension automatique et la restauration d'alimentation). Certains serveurs ne peuvent pas appliquer le délai dans le cas d'une restauration d'alimentation. Environ 10 secondes sont nécessaires au microprogramme iLO 2 avant que l'alimentation du serveur ne soit effective. Vous devez être doté du privilège Virtual Power and Reset (Alimentation et réinitialisation virtuelles) pour pouvoir modifier ce paramètre.

Paramètres d'alimentation du serveur

La fonction Power Regulator for ProLiant (Régulateur d'alimentation pour ProLiant) permet à iLO 2 de modifier de façon dynamique les niveaux de tension et fréquence du processeur selon les conditions de fonctionnement afin de permettre des économies d'énergie avec un impact minimum sur les performances. Les états de la tension et de la fréquence des processeurs prenant en charge la fonction de régulation sont prédéfinis et appelés *p-states*. Le logiciel peut faire basculer dynamiquement le processeur d'un état (p-state) à l'autre. P-0 est la combinaison fréquence/tension la plus élevée prise en charge par le processeur. La modification de l'état p-state du processeur en fonction de l'utilisation de l'unité centrale permet des économies d'énergie significatives avec un effet minimal sur les performances par réduction de la tension et de la fréquence du processeur lorsque le système est inactif, et par augmentation de la tension et de la fréquence du processeur en cas de besoin.

La page Power Management Settings (Paramètres de gestion de l'alimentation) permet de visualiser et contrôler le mode du régulateur de puissance du serveur. Vous devez disposer du droit de configuration des paramètres iLO 2 pour modifier ce paramètre.



- La section Power Regulator for ProLiant (Régulateur d'alimentation pour ProLiant) propose les options suivantes :
  - L'option Enable HP Dynamic Power Savings Mode (Activer le mode Alimentation dynamique HP) permet au processeur de définir lui-même le niveau d'alimentation en fonction de l'utilisation.
  - L'option Enable HP Static Low Power Mode (Activer le mode Alimentation faible HP) attribue au processeur la puissance minimale.
  - Le mode HP Static High Performance (Hautes performances statiques HP) affecte au processeur un état optimal et l'oblige à y rester.
  - Le mode Enable OS Control (Activer le contrôle du système d'exploitation) affecte au processeur la puissance maximale.

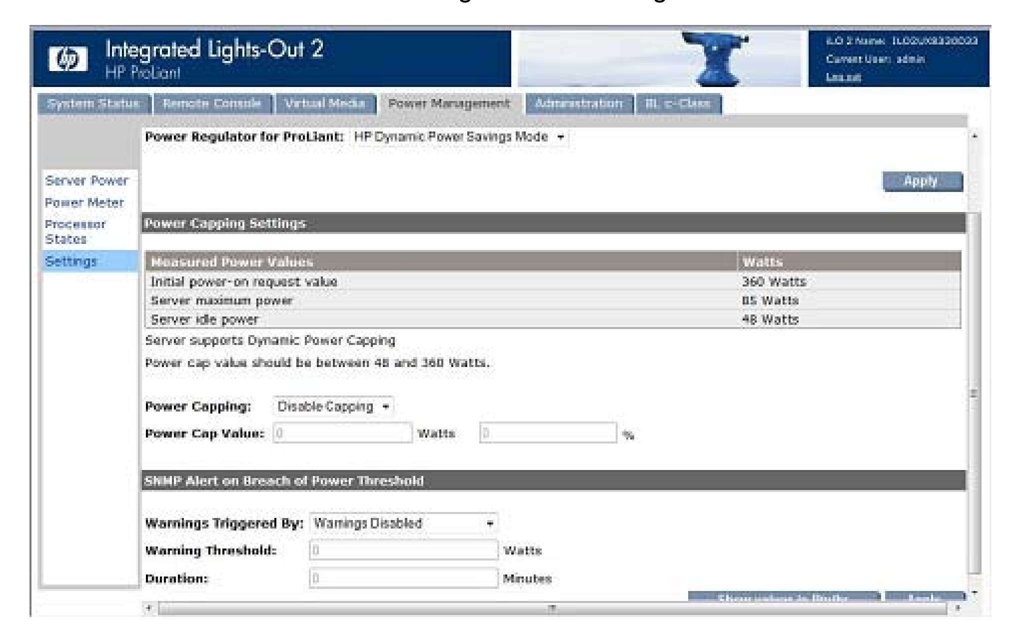
    Après avoir sélectionné une option Power Regulator for ProLiant (Régulateur d'alimentation pour ProLiant), cliquez sur **Apply** (Appliquer) pour enregistrer le paramètre. Le serveur doit être redémarré pour que la modification soit prise en compte. Ces paramètres ne peuvent pas être modifiés pendant l'auto-test de mise sous tension (POST) du serveur. Si, après avoir cliqué sur **Apply** (Appliquer), les paramètres ne sont pas modifiés, cela signifie que le serveur est peut-être en cours de démarrage ou doit être redémarré. Quittez tous les programmes RBSU ouverts, attendez la fin de l'auto-test, puis relancez l'opération.
- La section Power Capping Settings (Paramètres de limite de puissance) permet de visualiser les valeurs de puissance mesurées, ainsi que de définir et de désactiver une limite de puissance.

  Les valeurs de puissance mesurées incluent la valeur maximum d'alimentation du serveur, la puissance maximum du serveur et la puissance du serveur à l'état inactif. La valeur maximum d'alimentation correspond à la puissance maximum pouvant être fournie par l'alimentation du serveur. La puissance maximum du serveur et la puissance du serveur à l'état inactif sont déterminées grâce à deux tests de puissance exécutés par la ROM lors du POST.

  Power Cap Setting (Paramètre de limite de puissance) permet de définir une limite de puissance sur le serveur. Une fois la limite de puissance définie, la lecture de puissance moyenne sur le serveur en fonction du temps doit être inférieure ou égale à la valeur de la limite. Vous pouvez définir une limite de puissance en entrant une valeur exprimée soit en watt ou en BTU/heure (cliquez sur **Show values in Btu/hr** [Afficher les valeurs en BTU/heure]), soit en pourcentage.

Le pourcentage correspond à la différence entre la puissance maximum et la puissance à l'état inactif. La valeur de limite ne peut pas être inférieure à la puissance du serveur à l'état inactif.

Les paramètres de limitation de puissance sont désactivés lorsque le serveur fait partie d'une limitation dynamique de la puissance du boîtier. Ces valeurs sont définies et modifiées à l'aide de Onboard Administrator ou de Insight Power Manager.



- ◦ Si le serveur possède le matériel et le logiciel adaptés pour prendre en charge la limitation dynamique de la puissance, le message `System supports Dynamic Power Capping` (Le système prend en charge la limitation dynamique de la puissance) apparaît. La limitation dynamique de la puissance permet de protéger le circuit électrique à l'aide d'un disjoncteur.
- ◦ Si le message `System supports Dynamic Power Capping` (Le système prend en charge la limitation dynamique de la puissance) n'apparaît pas, cela signifie que le serveur prend en charge le système standard de limitation de la puissance. Le système standard de limitation de la puissance n'est pas suffisamment réactif pour assurer une protection à l'aide d'un disjoncteur.

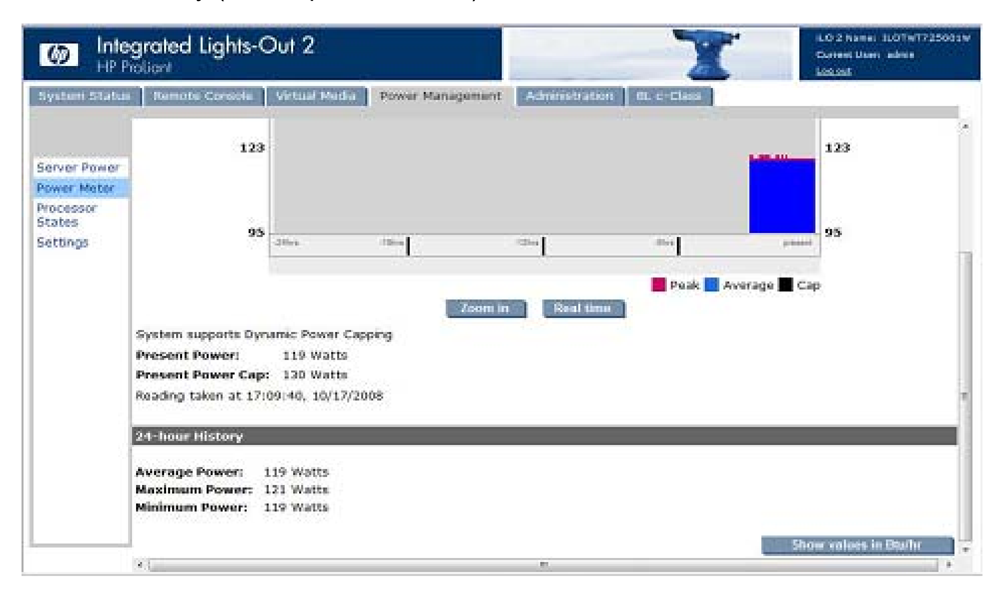
  Pour plus d'informations sur la limitation dynamique de la puissance, reportez-vous à la section « Limitation dynamique de la puissance pour les lames de serveur »

- Les alertes SNMP permettent d'avertir lorsque la consommation électrique dépasse un seuil donné. Vous pouvez configurer les paramètres suivants :
  - ◦ Déclenchement des avertissements - Permet de déterminer si les avertissements sont basés sur la consommation électrique maximale, sur la consommation électrique moyenne ou désactivés.
  - ◦ Seuil d'avertissement - Permet de définir le seuil de consommation électrique à partir duquel les alertes SNMP sont envoyées.
  - ◦ Durée - Permet de définir la durée (en minutes) pendant laquelle la consommation électrique doit rester supérieure au seuil d'avertissement avant le déclenchement d'une alerte SNMP. La durée maximale autorisée est de 240 minutes, et doit être un multiple de 5.

Pour utiliser les paramètres sélectionnés, cliquez sur **Apply** (Appliquer). Certains serveurs permettent la modification du niveau de puissance du processeur via le RBSU du système. Pour plus d'informations, reportez-vous au manuel de l'utilisateur de votre système.

Données relatives à la puissance du serveur

iLO 2 permet de visualiser graphiquement l'utilisation de la puissance du serveur. L'utilisation de la puissance du serveur est visualisée sur la page Power Meter Readings (Lectures du mesureur de puissance) sous forme de graphique. Pour accéder à la page Power Meter Readings (Lectures du mesureur de puissance), sélectionnez **Power Management** (Gestion de l'alimentation), puis cliquez sur **Power Meter** (Mesureur de puissance). La page Power Meter Readings (Lectures du mesureur de puissance) comporte deux sections : Power Meter Readings (Lectures du mesureur de puissance) et 24-Hour History (Historique 24 heures).



La section Power Meter Readings (Lecture du mesureur de puissance) affiche les informations suivantes :

- Le graphique des données affiche la consommation électrique du serveur au cours des dernières 24 heures. iLO 2 recueille les informations relatives à la consommation sur le serveur toutes les cinq minutes. Pour chaque intervalle de cinq minutes, la consommation électrique maximale et moyenne est stockée dans une mémoire tampon circulaire. Ces deux valeurs s'affichent sous la forme d'un graphique à barres, avec les valeurs moyennes en bleu et les valeurs maximales en rouge. Ces données sont remises à zéro à chaque réinitialisation du serveur ou de iLO 2.
  - Pour accroître la visibilité, cliquez sur **Zoom in** (Zoom avant), ce qui permet d'augmenter la largeur des barres sur le graphique de données d'alimentation. Un curseur apparaît dans ce mode pour permettre l'inspection des données dans une fenêtre de même taille.
  - Pour afficher l'utilisation actuelle de la puissance, cliquez sur **Real Time** (Temps réel). Le graphique des données Real Time (Temps réel) affiche les informations relatives à la consommation électrique (consommation maximale, consommation moyenne et limite de consommation) pour les dernières 20 minutes.
- La prise en charge actuelle de la limitation de puissance
- La valeur Present Power (Consommation électrique actuelle) affiche le niveau de consommation actuel sur le serveur.
- La valeur Present Power Cap (Limite de puissance actuelle) affiche la valeur actuelle de la limite de puissance.

La section 24-Hour History (Historique 24 heures) affiche les informations suivantes :

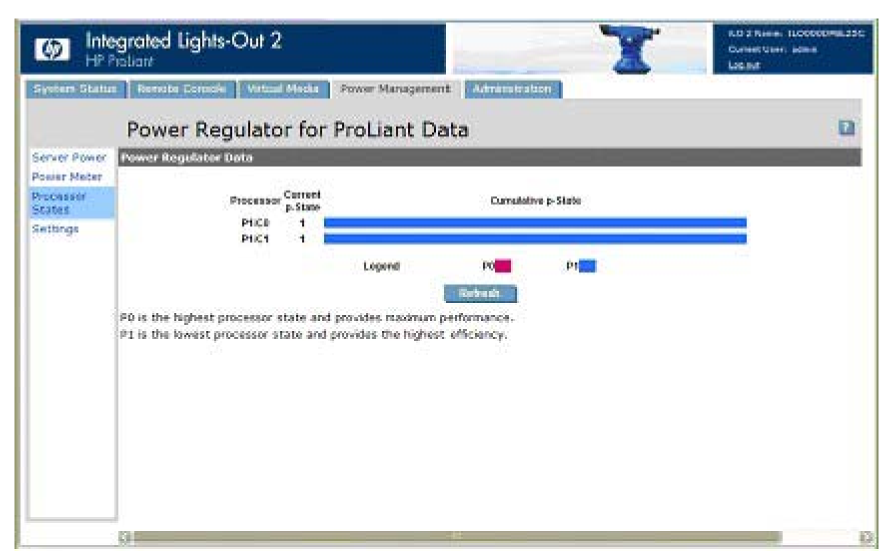
- La valeur Average Power Reading (Relevé moyen de la consommation électrique) affiche la moyenne des niveaux moyens d'alimentation sur le serveur au cours des dernières 24 heures. Si le serveur n'a pas fonctionné pendant 24 heures, la valeur est la moyenne de tous les relevés depuis l'amorçage du serveur.
- La valeur Maximum Power (Consommation électrique maximum) affiche le niveau maximal du relevé d'alimentation sur le serveur au cours des dernières 24 heures. Si le serveur n'a pas fonctionné pendant 24 heures, la valeur maximale de tous les relevés, depuis l'amorçage du serveur, s'affiche.
- La valeur Minimum Power (Consommation électrique minimale) affiche le niveau minimal du relevé d'alimentation sur le serveur au cours des dernières 24 heures. Si le serveur n'a pas fonctionné pendant 24 heures, la valeur est la valeur minimale de tous les relevés depuis l'amorçage du serveur.
- Show value in BTUs (Afficher les valeurs en BTU) permet de passer de l'affichage des données en watts à l'affichage des données en BTU.

États du processeur

La page Power Regulator for ProLiant Data (Données du régulateur de puissance pour ProLiant) permet de visualiser les états du processeur (p-state), ainsi qu'un pourcentage moyen de la durée pendant laquelle les processeurs logiques ont été définis sur chaque p-state au cours des dernières 24 heures. Cliquez sur **Refresh** (Actualiser) pour mettre à jour le graphique de données de p-state.

Vous devez disposer du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2) pour afficher la page Power Regulator for ProLiant Data (Données du régulateur de puissance pour ProLiant). Power Regulator for ProLiant Data (Données du régulateur de puissance pour ProLiant) est une fonction sous licence, disponible lors de l'achat de licences facultatives. Pour plus d'informations, reportez-vous à la section « Licence » (Licence à la page 21).

Pour afficher la page Power Regulator for ProLiant Data (Données du régulateur de puissance pour ProLiant), cliquez sur **Power Management>Processor States** (Gestion de l'alimentation >États des processeurs).



La page Power Regulator Data (Données du régulateur de puissance) affiche les données collectées concernant les p-state, depuis la mise sous tension de l'hôte, une fois par seconde et actualise l'affichage une fois toutes les 5 minutes. La ROM système lit l'état en cours de chaque processeur

logique. Le registre des états des plates-formes Intel® reflète la fréquence et la tension de fonctionnement actuelles. Étant donné le nombre des dépendances processeur, l'état peut ou non refléter un p-state absolu. Il se peut que la fréquence soit à un p-state donné et la tension à un p-state plus élevé. La ROM système met à jour le décompte p-state de la fréquence actuelle et non la tension.

Les données sont affichées sous la forme d'un graphique à barres dont la longueur totale représente 100 % du temps couvert par les données. Un graphique de données est affiché pour chaque processeur ou objet central. Aucun graphique de données n'est affiché pour les threads multiples d'un processeur ou d'un objet central compatible avec la technologie Hyper-Threading. La barre comporte des portions de couleurs différentes pour chaque p-state rencontré par le processeur, chaque portion de couleur étant proportionnée pour représenter le pourcentage du temps total passé par le processeur dans un état donné. Si vous placez le curseur de la souris sur le graphique à barres, une info-bulle indiquant le pourcentage correspondant à la partie de la barre s'affiche.

Efficacité de l'alimentation

iLO 2 permet de mettre en oeuvre une utilisation améliorée de l'alimentation à l'aide d'un mode HEM (High Efficiency Mode - Mode haute efficacité). Le mode HEM améliore l'efficacité de l'alimentation du système en plaçant les blocs d'alimentation secondaires en mode par palier. Lorsque les blocs d'alimentation secondaires sont en mode par palier, les blocs d'alimentation principaux fournissent toute l'alimentation continue au système. Les blocs d'alimentation sont plus efficaces (plus de watts de sortie CC pour chaque watt d'entrée CA) à des niveaux de sortie d'alimentation plus élevés et l'efficacité de l'alimentation globale s'en trouve améliorée.

Lorsque le système commence à tirer plus de 70 % de capacité de la sortie d'alimentation maximum des blocs d'alimentation principaux, les blocs d'alimentation secondaires reviennent à un fonctionnement normal (sortie du mode par palier). Lorsque l'usage d'alimentation descend au-dessous de 60 % de la capacité des blocs d'alimentation principaux, les blocs d'alimentation secondaires retournent en mode par palier. Le mode HEM permet d'atteindre une consommation d'alimentation égale à la sortie d'alimentation maximum des blocs d'alimentation principaux et secondaires, tout en maintenant une efficacité améliorée à des niveaux d'utilisation d'alimentation inférieurs.

Le mode HEM n'affecte pas la redondance de l'alimentation. En cas de panne des blocs d'alimentation principaux, les blocs d'alimentation secondaires commencent immédiatement à fournir une alimentation continue au système, empêchant ainsi tout arrêt.

Vous pouvez configurer le mode HEM uniquement au travers de l'utilitaire RBSU. Vous ne pouvez pas modifier ces paramètres via iLO. Les paramètres du mode HEM sont Enabled (Activé) et Disabled (Désactivé) (également appelé Mode équilibré), et Odd (Impaires) ou Even (Paires) pour les blocs d'alimentation principaux. Ces paramètres sont visibles dans la section High Efficiency Mode & Standby Power Save Mode de l'onglet System Information>Power (Informations système>Alimentation). Cette section affiche les informations suivantes :

- Si le mode HEM est activé ou désactivé
- Quels blocs d'alimentation sont principaux (si le mode HEM est activé)

- Quels blocs d'alimentation ne prennent pas en charge le mode HEM



Arrêt automatique sans perte de données

La capacité du microprocesseur iLO 2 d'effectuer un arrêt sans perte de données exige la coopération du système d'exploitation. Pour un arrêt de ce type, le driver d'état doit être chargé. iLO 2 communique avec ce dernier, et la méthode adéquate utilisée par le système d'exploitation pour fermer le système en toute sécurité tout en assurant l'intégrité des données est mise en œuvre.

Dans les cas où le driver d'état n'est pas chargé, le processeur iLO 2 tente d'utiliser le système d'exploitation pour effectuer un arrêt sans perte de données depuis le bouton d'alimentation. iLO 2 émule une pression physique sur celui-ci pour obtenir du système d'exploitation un arrêt en bonne et due forme. Le comportement du système d'exploitation dépend de la configuration et du paramétrage définis pour une pression sur le bouton d'alimentation.

La configuration EAAS (Environment Abnormality Auto-Shutdown – Fermeture automatique pour anomalie relative à l'environnement) du RBSU (Rom-Based Setup Utility – Utilitaire de configuration basé sur la mémoire morte) de la ROM hôte permet de désactiver la fonction d'arrêt automatique. Cette configuration permet de désactiver l'arrêt automatique sauf dans les conditions les plus extrêmes susceptibles d'entraîner des dommages physiques.

Sous Windows Server® 2003, la stratégie de groupe de l'ordinateur désactive l'arrêt automatique du système sans perte de données en effectuant une pression brève, à moins qu'un administrateur ne soit connecté au système d'exploitation. Pour modifier ce paramètre et activer l'arrêt automatique sans perte de données, effectuez les opérations suivantes :

1. Depuis une invite de commande, exécutez la commande `gpedit.misc`.

2. Définissez Configuration ordinateur>Paramètres Windows>Paramètres de sécurité>Stratégies locales>Options de sécurité>Arrêt : permettre au système d'être arrêté sans avoir à se connecter sur **Activé**.

Supervision avancée des serveurs ProLiant BL p-Class

iLO 2 Advanced est un composant standard des lames de serveur ProLiant BL p-Class qui assure l'intégrité du serveur et permet de le superviser aisément à distance. Ses fonctionnalités sont

accessibles à partir d'un périphérique client réseau à l'aide d'un navigateur Web pris en charge. En outre, iLO 2 Advanced offre des fonctionnalités de clavier, de souris et de vidéo (texte et graphique) à un serveur lame, quel que soit l'état du système d'exploitation hôte ou du serveur lame hôte.

Le système iLO 2 comprend un microprocesseur intelligent, une mémoire sécurisée et une interface réseau dédiée. Cette conception le rend indépendant du serveur hôte et de son système d'exploitation. iLO 2 permet d'accéder à distance à tout client réseau autorisé, envoie des alertes et fournit d'autres fonctionnalités de supervision de serveur lame.

À l'aide d'un navigateur compatible, vous pouvez effectuer les tâches suivantes :

- Accéder à distance à la console de la lame de serveur hôte, notamment à tous les écrans en mode texte et en mode graphique, et à toutes les commandes de clavier et de souris.
- Mettre la lame de serveur hôte sous et hors tension à distance ou la redémarrer.
- Démarrer un serveur lame hôte à distance sur une image de disquette virtuelle pour effectuer une mise à niveau de la ROM ou pour installer un système d'exploitation.
- Envoyer des alertes à partir d'iLO 2 Advanced, quel que soit l'état de la lame de serveur hôte.
- Accéder aux fonctionnalités avancées de résolution des problèmes fournies par iLO 2 Advanced.
- Lancer un navigateur Web, utiliser les alertes SNMP et diagnostiquer le serveur lame à l'aide de HP Systems Insight Manager.
- Configurer des paramètres de compartiment IP statique pour les cartes réseau de supervision iLO 2 dédiées sur chaque lame de serveur d'un boîtier pour un déploiement plus rapide.

La lame de serveur doit être correctement connectée pour assurer la connectivité iLO 2. Connectez-vous à la lame de serveur en utilisant l'une des méthodes suivantes :

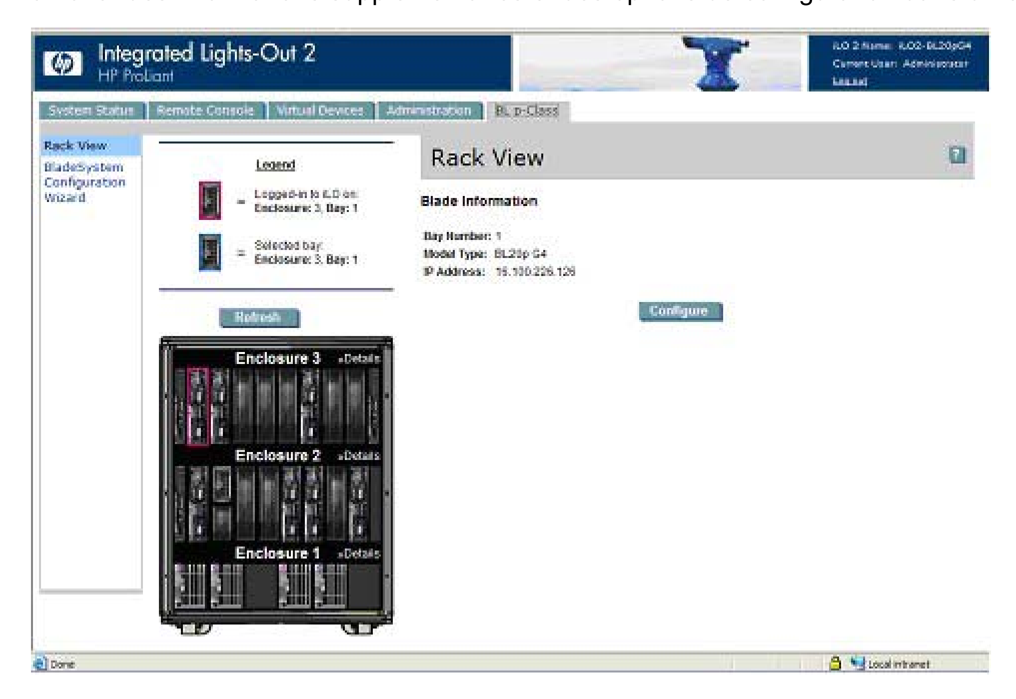
- Via un réseau existant (dans le rack) : cette méthode nécessite d'installer la lame de serveur dans son boîtier et de lui affecter une adresse IP (manuellement ou via DHCP).
- Via le port d'E/S du serveur lame
  - Dans le rack : cette méthode nécessite de connecter le câble d'E/S local au port d'E/S et à un PC client. À l'aide de l'adresse IP fixe inscrite sur l'étiquette du câble d'E/S et des informations d'accès initial à l'avant de la lame de serveur, vous pouvez accéder à la lame de serveur avec la console distante iLO 2 Advanced.
  - Hors du rack, à l'aide de la station de diagnostic : cette méthode nécessite la mise sous tension de la lame de serveur avec la station de diagnostic en option et la connexion à un ordinateur externe à l'aide de l'adresse IP fixe et du câble d'E/S local. Pour les instructions de câblage, reportez-vous à la documentation livrée avec la station de diagnostic ou au CD Documentation.
  - Via les connecteurs du panneau arrière de la lame de serveur (hors du rack, à l'aide de la station de diagnostic) : cette méthode permet de configurer une lame de serveur hors du rack en l'alimentant à l'aide de la station de diagnostic et en la connectant à un réseau existant via un hub. L'adresse IP est attribuée par un serveur DHCP présent sur le réseau.

L'onglet BL p-Class permet de contrôler des paramètres propres au rack des serveurs lame ProLiant BL p-Class. La carte iLO 2 propose également des diagnostics basés sur le Web pour le rack des serveurs ProLiant BL p-Class.

Vue du rack

La page Rack View (Afficher rack) présente les boîtiers ainsi que leurs serveurs lame, composants réseau et modules d'alimentation. Tout composant présent dans le rack est affiché et peut être

sélectionné à la page Rack View. Vous ne pouvez pas sélectionner les compartiments vides. Les informations propres au composant, comme le nom du serveur lame, l'adresse IP et le type de produit, s'affichent lorsque vous positionnez le curseur sur chaque composant. Cliquez sur le composant pour afficher des informations supplémentaires et des options de configuration dans un écran.



Les champs suivants sont accessibles à partir de l'écran Rack View (Afficher rack) :

- Nom du rack
- Logged-in iLO Location (Emplacement iLO intégré)

  Cette section annote la lame à laquelle vous êtes connecté. Vous ne pouvez configurer les paramètres d'aucune autre lame.
- Selected Bay Location (Emplacement compartiment sélectionné)

  Cette section annote le compartiment sélectionné. Vous pouvez visualiser les données des différents types de composants, comme les lames, les blocs d'alimentation, les composants réseau et les boîtiers.
- Enclosure Details (Détails boîtier)

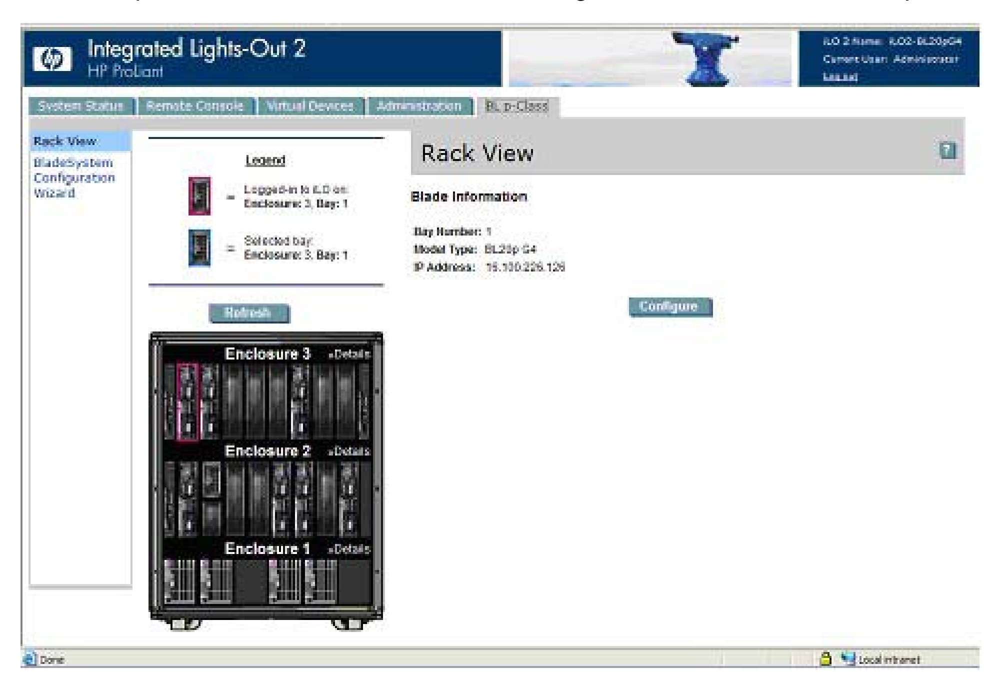
  Pour afficher des informations sur un boîtier donné, sélectionnez **Details** (Détails) sur les en-têtes de boîtier répertoriés.

Le bouton Refresh (Actualiser) permet d'obtenir des informations sur l'écran Rack View (Afficher rack). Cliquez sur **Refresh** (Actualiser) pour forcer une nouvelle représentation graphique du rack. Cette opération prendra quelques instants.

Si des informations erronées s'affichent dans l'écran Rack View, un message d'erreur apparaît à la place des composants. Vous pouvez de nouveau cliquer sur le bouton Refresh (Actualiser) pour tenter d'afficher les données correctes dans l'écran Rack View. Pour un meilleur affichage, la fonctionnalité Rack View requiert l'utilisation de la version 2.10 ou ultérieure du microprogramme Server Blade et Power Management Module.

Configuration et informations relatives à la lame

L'option de configuration de la lame fournit des informations sur l'identité, l'emplacement et l'adresse réseau de la lame sélectionnée sur la page Rack View (Afficher rack). Pour afficher ces paramètres, sélectionnez un composant de la lame, puis choisissez **Configurer** (Configurer) dans la page Rack View (Afficher Rack) (Vue du rack à la page 136). Vous pouvez modifier certains des paramètres de la lame à laquelle vous êtes connectée. Pour enregistrer ces modifications, cliquez sur **Apply** (Appliquer).



Les champs disponibles sont les suivants :

- Identification Information (Informations d'identification)
  - Bay Name (Nom du compartiment)
  - Bay Number (Numéro de baie)
- Power On Control (Bouton de mise sous tension)
  - Power Source (Source d'alimentation)
  - Enable Automatic Power On (Activer la mise sous tension automatique)
  - Enable Rack Alert Logging (IML) (Activer la consignation des alertes du rack - IML)

Informations relatives au boîtier



Les informations relatives au boîtier sont spécifiques au boîtier sélectionné. Pour afficher des informations sur un boîtier donné, sélectionnez **Details** (Détails) sur les en-têtes de boîtier répertoriés. Une quantité limitée d'informations, notamment le nom et le numéro de série, est disponible sur le rack.

Des informations de base sont disponibles pour les boîtiers ne contenant pas la lame à laquelle vous êtes connecté. Ces informations comprennent, notamment, le nom, le numéro de série et le type du boîtier.

Certains détails sont disponibles pour le boîtier contenant la lame à laquelle vous êtes connecté, notamment :

- Nom
- Serial number (Numéro de série)
- Enclosure Type (Type de boîtier)
- Firmware Revision (Révision du microprogramme)
- Hardware Revision (Révision du matériel)
- Température du boîtier
- Management Module UID (ID unique module de gestion)

Vous pouvez mettre à jour certains champs à l'aide du bouton **Apply** (Appliquer).

Informations relatives au boîtier d'alimentation

La page Power Enclosure Information (Informations relatives au boîtier d'alimentation) fournit des informations de diagnostic sur le module PMM et les composants contenus dans le boîtier d'alimentation. Ces informations offrent un aperçu de l'état de marche du boîtier et des composants d'alimentation.



Les champs disponibles sont les suivants :

- Nom du rack
- Rack serial number (Numéro de série du rack)
- Nom du boîtier
- Enclosure serial number (Numéro de série du boîtier)
- Enclosure Type (Type de boîtier)
- Firmware Revision (Révision du microprogramme)
- Hardware Revision (Révision du matériel)
- Load Balance Wire (Canal balance de charge)
- Température du boîtier
- Enclosure Temperature Side A and B (Température du boîtier face A et B)
- Management Module UID (ID unique module de gestion)

Vous pouvez mettre à jour certains champs à l'aide du bouton **Apply** (Appliquer).

Informations relatives aux composants réseau

Ces informations affichent l'état du panneau à interconnexions qui a été sélectionné. Les informations affichées comprennent le fusible A, le fusible B et le type de composant réseau.

Contrôle par la carte iLO 2 des voyants du serveur ProLiant BL p-Class

La carte iLO 2 supervise les serveurs BL p-Class via le suivi des messages POST et le voyant d'état du serveur.

Suivi des messages POST de serveur

Les possibilités de feedback sont limitées pendant l'amorçage du serveur étant donné la structure non centralisée des serveurs ProLiant BL p-Class. La carte iLO 2 propose un feedback au moment de l'amorçage en faisant clignoter le voyant vert de supervision du serveur pendant le test POST. Le voyant devient orange et ne clignote plus si l'amorçage échoue. Il devient vert et cesse de clignoter lorsque l'amorçage est réussi.

Après un amorçage réussi, le contrôle du voyant d'état du serveur est renvoyé au serveur, qui peut alors l'éteindre ou en modifier la couleur pour indiquer le bon état de fonctionnement du matériel.

Notification d'alimentation insuffisante

La carte iLO 2 allume le voyant d'état du serveur en rouge si elle ne parvient pas à le mettre sous tension en raison d'une alimentation insuffisante dans l'infrastructure du rack.

Transfert des alertes ProLiant BL pClass

La carte iLO 2 prend en charge les traps (alertes) SNMP de l'infrastructure lame grâce à la fonction pass-through. La prise en charge du système d'exploitation n'est pas nécessaire pour que la carte iLO 2 indique l'état de l'infrastructure lame. Les traps sont générés par Enclosure Manager (Gestionnaire du boîtier) et Power Supply Manager (Gestionnaire de l'alimentation) et sont transmis à la carte iLO 2. Le microprogramme pClass transfère les alertes relatives à l'infrastructure sous forme de traps SNMP vers une console de supervision correctement configurée. Ces messages permettent à la console de supervision SNMP de contrôler les alertes pClass.

Le transfert des alertes pClass est désactivé par défaut. Cette fonction peut être activée depuis la page Web SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager).

Les alertes suivantes sont identifiées et transférées par la carte iLO 2 :

ID de l'alerte	Description
22005	Erreur de température du boîtier
22006	Température du boîtier anormale
22007	Température du boîtier OK
22008	Panne du ventilateur du boîtier
22009	Mauvais fonctionnement du ventilateur du boîtier
22010	Ventilateur du boîtier OK
22013	Coupure de l'alimentation du rack
22014	Alimentation du rack défectueuse
22015	Alimentation du rack OK
22023	Panne du rack serveur : alimentation insuffisante

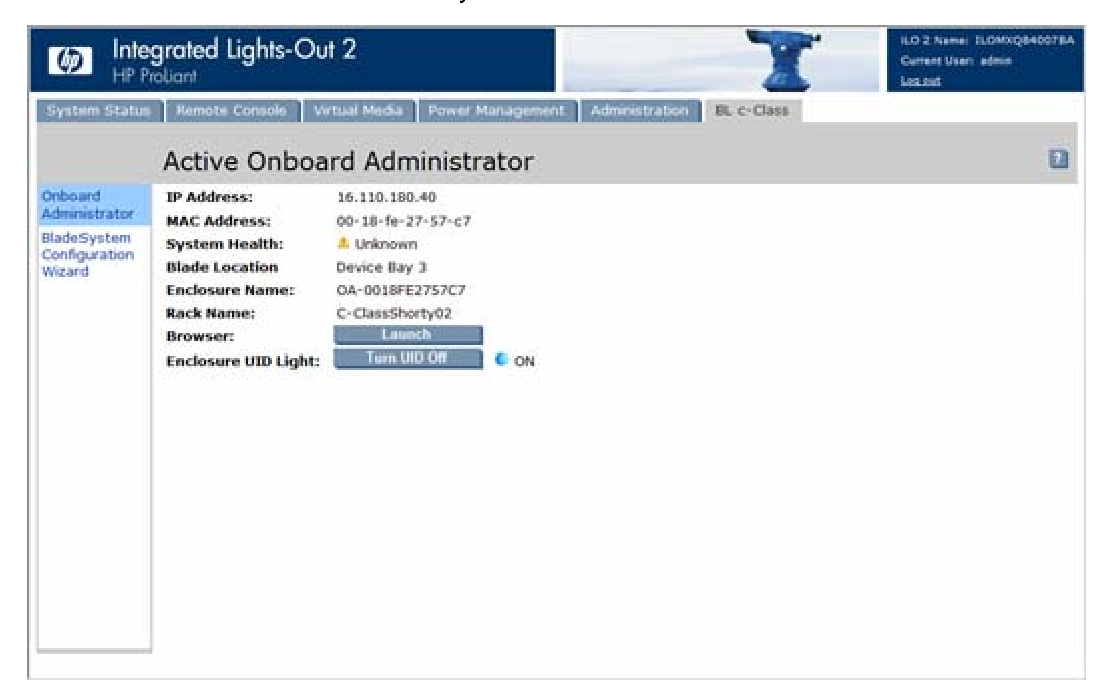
ProLiant BladeSystem HP Onboard Administrator (Administrateur intégré HP ProLiant BladeSystem)

HP BladeSystem Onboard Administrator (Administrateur intégré HP ProLiant BladeSystem) est le processeur de supervision, le sous-système et le microprogramme du boîtier utilisé pour prendre en charge HP BladeSystem et tous les périphériques gérés contenus dans le boîtier.

Vous pouvez accéder à iLO 2 depuis l'option iLO de HP Onboard Administrator (iLO option à la page 146), directement ou en utilisant le lien Web Administration (Administration Web)(Web Administration (Administration Web) à la page 147). Pour plus d'informations sur la connexion directe à iLO 2, reportez-vous à la section « Première connexion à iLO 2 » (Première connexion à iLO 2 à la page 13).

Onglet BL c-Class de iLO 2

L'onglet BL c-Class de l'interface Web de iLO 2 permet d'accéder à Onboard Administrator et à BladeSystem Configuration Wizard (Assistant de configuration BladeSystem). Pour plus d'informations sur BladeSystem Configuration Wizard (Assistant de configuration BladeSystem), reportez-vous au *Manuel de l'utilisateur de HP BladeSystem Onboard Administrator*.



L'option Onboard Administrator permet d'afficher un brève présentation de l'état du système du serveur et de lancer un navigateur (qui ouvre l'écran HP Onboard Administrator Rack View [Affichage du rack de l'Administrateur intégré HP]) ou d'activer/désactiver le voyant UID.

Adressage IP du boîtier

Au cours de l'exécution de First Time Setup Wizard (Assistant Première configuration), vous êtes invité à configurer l'adressage IP du boîtier. Pour plus d'informations sur la procédure de configuration complète de l'assistant, reportez-vous au *Manuel de l'utilisateur de HP BladeSystem Onboard Administrator*.

Les ports iLO 2 de la lame de serveur et les ports de supervision du module à interconnexions peuvent obtenir les adresses IP du réseau de supervision de trois manières : adresse DHCP, adresse IP statique ou EBIPA. Si votre réseau dispose d'un service DHCP externe ou si vous souhaitez affecter

manuellement des adresses IP statiques une par une sur les lames de serveur et les modules d'interconnexions, cliquez sur **Skip** (Ignorer) pour sauter cette étape.

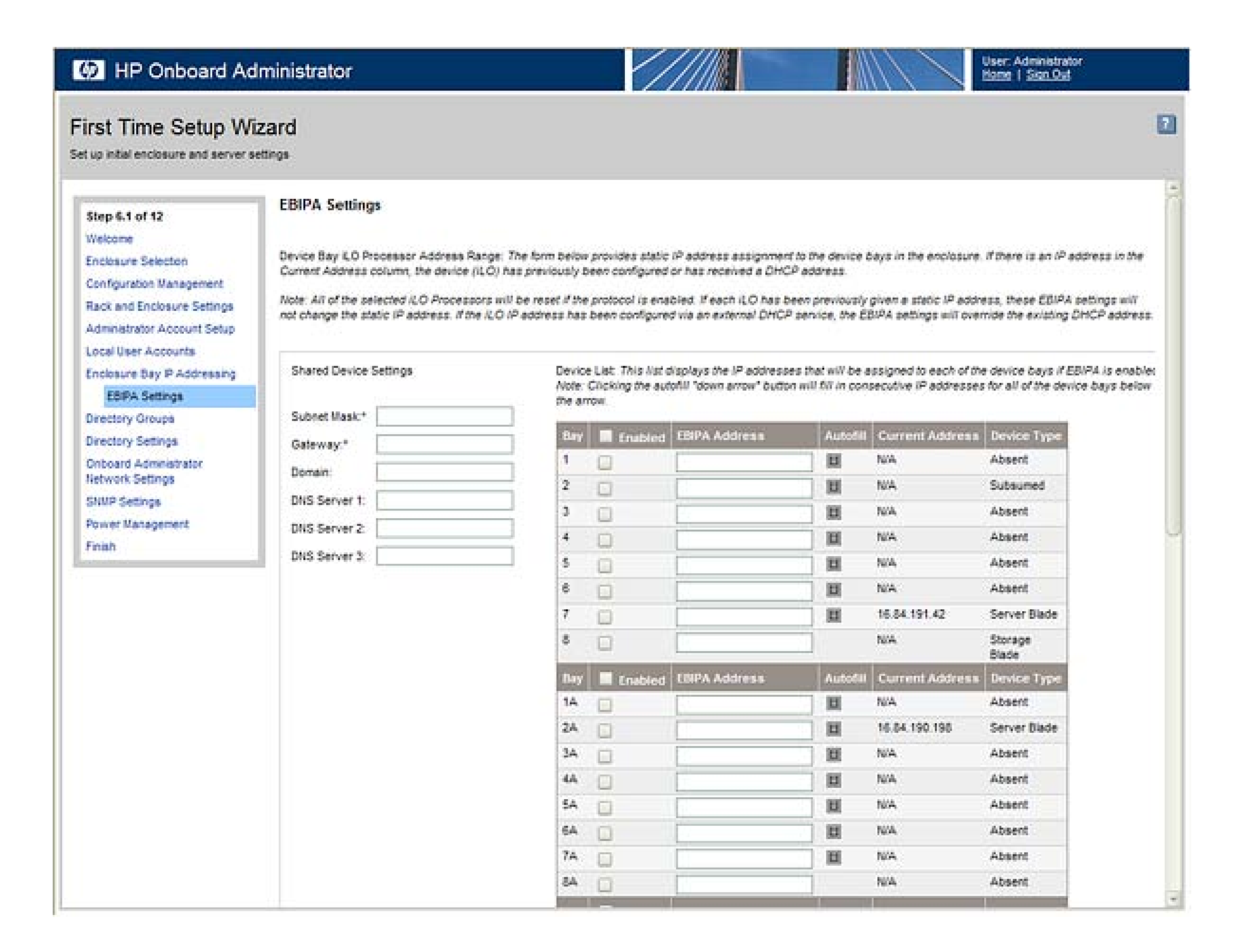
- Adresses DHCP : le système iLO 2 des lames de serveur utilise par défaut l'adressage DHCP, qu'il obtient via le connecteur réseau du module Onboard Administrator actif. Les modules à interconnexions disposant d'une connexion réseau de supervision à Onboard Administrator peuvent également choisir l'adresse DHCP par défaut.

  L'interface graphique utilisateur Onboard Administrator répertorie l'adresse IP du port iLO 2 de la lame de serveur et du port de supervision du module à interconnexions.

- Adresse IP statique
  - Manuel : si votre installation préfère l'attribution d'adresses IP statiques, vous pouvez attribuer une par une des adresses statiques uniques à chacun des ports iL0 2 des lames de serveur et de gestion des modules d'interconnexion. Vous pouvez également utiliser l'EBIPA pour attribuer une plage d'adresses IP statiques à chaque baie de lame de serveur et de module d'interconnexion.
  - EBIPA : lorsqu'une lame de serveur ou un module d'interconnexion est inséré dans une baie où EBIPA est activé, ce port de supervision obtiendra l'adresse IP statique spécifique du module Onboard Administrator si ce périphérique est configuré pour DHCP.

L'administrateur définit une plage indépendante de baies de lames de serveur et de baies de modules d'interconnexion à l'aide de l'assistant de configuration EBIPA du Onboard Administrator. La première adresse d'une plage est attribuée à la première baie et les adresses suivantes de la plage aux baies suivantes.

Ainsi, si vous définissez la plage EBIPA des baies de serveur entre 16.100.226.21 et 16.100.226.36, le serveur iLO 2 de la première baie de serveur se voit attribuer l'adresse 16.100.226.21, et le serveur iLO 2 de la douzième baie de serveur prend l'adresse 16.100.226.32. Si vous définissez la plage EBIPA des baies d'interconnexion entre 16.200.139.51 et 16.200.139.58, le port de gestion du module d'interconnexion de la première baie est alors défini sur 16.200.139.51 et le port de gestion du module d'interconnexion de la septième baie sur 16.200.139.57.



Pour activer les paramètres EBIPA pour les baies de serveur du boîtier, sélectionnez **Enable Enclosure Bay IP Addressing for Server Bay iLO 2 Processors** (Activer l'adressage IP des compartiments de boîtier pour les processeurs iLO 2 de la baie de serveur), puis entrez les informations suivantes :

Champ	Valeur possible	Description
Beginning Address (Adresse de début)	###.###.###.### où ### est compris entre 0 et 255	Adresse IP de début des baies de serveur ou d'interconnexion. Cliquez sur la flèche en regard du champ Beginning Address (Adresse de début), puis cliquez sur **Update List** (Actualiser la liste) pour actualiser la liste de périphériques ou la liste d'interconnexions
Subnet Mask (Masque de sous-réseau)	###.###.###.### où ### est compris entre 0 et 255	Masque de sous-réseau des baies de serveur ou d'interconnexion
Gateway (Passerelle)	###.###.###.### où ### est compris entre 0 et 255	Adresse de passerelle des baies de serveur ou d'interconnexion
Domain (Domaine)	Une chaîne de caractères, y compris tous les caractères alphanumériques et le tiret (-)	Nom de domaine des baies de serveur ou d'interconnexion
DNS Server 1 (Serveur DNS 2)	###.###.###.### où ### est compris entre 0 et 255	Adresse IP pour le serveur DNS primaire
DNS Server 2 (Serveur DNS 2)	###.###.###.### où ### est compris entre 0 et 255	Adresse IP pour le serveur DNS secondaire

Champ	Valeur possible	Description
DNS Server 3 (Serveur DNS 2)	###.###.###.### où ### est compris entre 0 et 255	Adresse IP pour le serveur DNS tertiaire
NTP Server 1 (Serveur NTP 2	###.###.###.### où ### est compris entre 0 et 255	Adresse IP du serveur principal utilisé pour synchroniser la date et l'heure à l'aide du protocole NTP
NTP Server 2 (Serveur NTP 2	###.###.###.### où ### est compris entre 0 et 255	Adresse IP du serveur secondaire utilisé pour synchroniser la date et l'heure à l'aide du protocole NTP

Limitation dynamique de la puissance pour les lames de serveur

La limitation dynamique de la puissance est une fonction de iLO 2, disponible pour les lames de serveur c-Class et accessible depuis HP Onboard Administrator. Pour plus d'informations sur l'ensemble des options de paramètres de puissance des lames de serveur c-Class, reportez-vous au *Manuel de l'utilisateur de HP BladeSystem Onboard Administrator*.

La limitation dynamique de la puissance fonctionne seulement si les versions de la plate-forme matérielle de votre système, du BIOS (ROM) et du microprogramme de microcontrôleur d'alimentation prennent en charge la limitation avancée de la puissance. Si votre système possède les capacités requises pour exécuter une limitation avancée de la puissance, iLO 2 fonctionne automatiquement en mode limitation dynamique de la puissance.

Deux options de limitation dynamique de la puissance sont disponibles dans Onboard Administrator (Administrateur intégré) :

- Dynamic Power (Alimentation dynamique)

  S'il est activé, le mode d'alimentation dynamique place les alimentations inutilisées en mode Standby afin d'accroître l'efficacité de l'alimentation du boîtier et de réduire la consommation électrique du boîtier pendant les demandes plus faibles d'alimentation. L'augmentation de la demande en alimentation entraîne automatiquement le passage en mode pleinement opérationnel des alimentations en attente. Si l'alimentation dynamique est :

  - Enabled (Activée) (paramètre par défaut) : certaines alimentations peuvent être placées automatiquement en mode Standby, afin d'améliorer l'efficacité globale du sous-système d'alimentation du boîtier.
  - Disabled (Désactivée) : toutes les alimentations partagent la charge. L'efficacité du sous-système d'alimentation varie en fonction de la charge.

- Enclosure Dynamic Power Cap (Limitation dynamique de la puissance du boîtier)

  Paramètre facultatif, qui vous permet de définir une limite pour un groupe de serveurs situés dans un même boîtier. La limite définie doit être comprise entre les valeurs affichées au-dessus du champ Enclosure Dynamic Power Cap (Limitation dynamique de la puissance du boîtier). Ces valeurs sont calculées en fonction de la configuration du boîtier.

  Lorsque les serveurs fonctionnent, la demande en puissance varie en fonction de chaque serveur. Une limite de puissance est définie pour chaque serveur. Elle est suffisante pour lui permettre de faire face à sa charge de travail, mais reste conforme à la limitation dynamique de la puissance du boîtier.

Vous pouvez utiliser indifféremment la limitation statique de la puissance ou la limitation dynamique de la puissance du boîtier dans les situations suivantes :

- Si l'alimentation de l'installation se limite au boîtier, vous pouvez entrer une limite fixe dans chaque boîtier. Par exemple, si l'installation hébergée limite le boîtier à 5 000 W, entrez 5000 dans le champ Limit Enclosure Input Watts. Le module Onboard Administrator limite alors l'attribution totale d'alimentation à 5 000 W, ce qui peut avoir pour conséquence de refuser l'alimentation de certaines lames de serveur.
- Si l'installation limite la capacité de refroidissement du boîtier, divisez par 3,41 la limite de la valeur Btu/hr disponible pour le boîtier afin de déterminer la limite en watts pour ce boîtier. Entrez la limite en watts afin de restreindre la charge calorifique des boîtiers. Par exemple : L'installation limite un boîtier individuel à 27 280 Btu/hr, puis la division de 27 280 par 3,41 donne 8 000 W. Entrez cette limite de puissance en watts pour limiter ce boîtier à 27 280 BTU/hr. Cette limite peut avoir pour conséquence le refus d'alimenter certaines lames de serveur.
- La méthode de limitation dynamique de la puissance du boîtier est recommandée lorsque vous devez limiter la charge électrique ou la sortie thermique d'un boîtier. Comparée à la limitation statique de la puissance, elle autorise la mise sous tension d'un plus grand nombre de lames. La méthode de limitation statique est recommandée dans les cas suivants :

  — Vous ne souhaitez pas que des limites soient réglées de façon dynamique sur vos lames de serveur.

  — Vous préférez ne pas mettre une lame de serveur sous tension si elle ne peut atteindre sa puissance maximale (même si cette solution est généralement moins consommatrice d'énergie).

  — Plus d'1/4 des lames du boîtier ne possèdent pas la configuration matérielle ou logicielle requise pour la limitation dynamique de la puissance du boîtier.

  — Vous ne possédez pas de bloc d'alimentation alternative redondant.

  — Ne définissez pas de limite si le boîtier est vide. Cela désactive à la fois la limitation statique de la puissance et la limitation dynamique de la puissance du boîtier.

Pour plus d'informations sur la limitation statique de la puissance, reportez-vous au *Manuel de l'utilisateur de HP BladeSystem Onboard Administrator*.

Ventilateur virtuel iLO 2

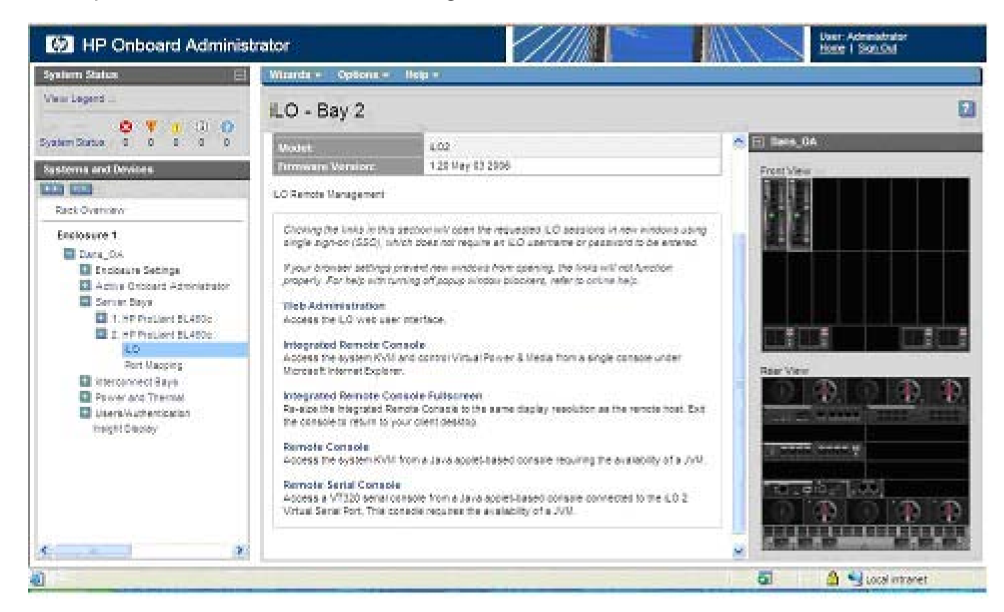
Dans les serveurs lame c-Class, HP Onboard Administrator contrôle les ventilateurs des boîtiers. Le microprogramme iLO 2 ne peut pas détecter ces ventilateurs de boîtier. Cependant, le microprogramme contrôle la température ambiante via un capteur situé sur le serveur lame. Les informations s'affichent sur l'interface iLO 2 et sont récupérées régulièrement par Onboard Administrator. Onboard Administrator utilise les informations du capteur collectées par l'ensemble des processeurs de supervision iLO 2 dans le boîtier afin de déterminer les vitesses des ventilateurs de boîtier.

iLO option

L'option iLO de HP Onboard Administrator vous permet d'accéder aux services suivants de iLO 2 : Web Administration (Administration Web) (Web Administration (Administration Web) à la page 147), Integrated Remote Console Fullscreen (Mode plein écran de la console distante intégrée) (Mode plein écran de l'IRC à la page 95), Integrated Remote Console (Console distante intégrée) (Option Integrated Remote Console (Console distante intégrée) à la page 96), Remote Console (console distante) et Remote Serial Console (Console série distante) (Remote Serial Console (Console série distante) à la page 112). Lorsque vous cliquez sur les liens de cette section, les sessions iLO 2 demandées

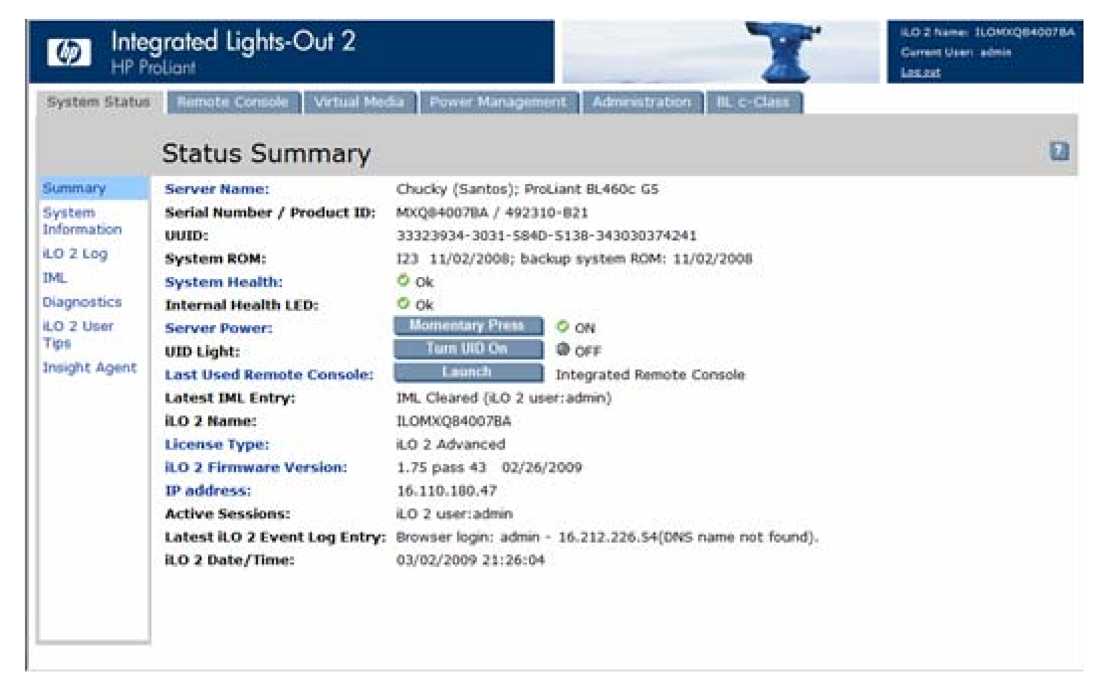
s'ouvrent dans de nouvelles fenêtres à l'aide de SSO, qui ne nécessite pas de saisie de nom d'utilisateur ni de mot de passe iLO 2.

Si les paramètres de votre navigateur empêchent l'affichage de nouvelles fenêtres, les liens ne fonctionneront pas correctement. Pour obtenir de l'aide sur la désactivation des bloqueurs de fenêtres intempestives, consultez l'aide en ligne.



Web Administration (Administration Web)

Le lien Web Administration (Administration Web) de l'interface HP Onboard Administrator permet d'accéder à l'interface utilisateur graphique de iLO 2. La page System Status (État du système) s'affiche avec une présentation de l'état du serveur.



Fonctionnalités de BL p-Class et de BL c-Class

Les serveurs HP ProLiant BL p-Class et ProLiant c-Class ont des fonctionnalités communes. Les différences sont présentées dans le tableau suivant :

Élément	BL c-Class	BL p-Class
Communications entre boîtiers	Ethernet	i2c
Adressage IP basé sur les boîtiers	DHCP	SBIPC
Authentification des boîtiers sur iLO 2	Mutuelle	Non prise en charge
Ventilateur du serveur	Virtuel	Physique
Informations et configuration du serveur lame	Illimitées	Limitées
Neutralisation de la mise sous tension	Non prise en charge	Prise en charge
Clé électronique frontale	SUV (sans iLO 2)	SUVi
Gestion des racks	Prise en charge complète via HP Onboard Administrator (Administrateur intégré HP)	Prise en charge limitée via iLO 2

5 Services d'annuaire

Cette section traite des rubriques suivantes :

Présentation de l'intégration d'annuaire

iLO 2 peut être configuré afin d'utiliser un annuaire pour authentifier et autoriser ses utilisateurs. Avant de configurer iLO 2 pour les annuaires, vous devez décider si vous souhaitez utiliser l'option de schéma HP Extended.

Les avantages de l'option du schéma HP Extended sont les suivants :

- Vous disposez d'une souplesse beaucoup plus grande concernant le contrôle de l'accès. Par exemple, l'accès peut être restreint à une tranche horaire dans la journée ou à une certaine plage d'adresses IP.
- Les groupes sont gérés dans l'annuaire et non dans chaque iLO 2.
- RILOE et RILOE II fonctionnent uniquement avec le schéma HP Extended (l'option sans schéma sera ajoutée à RILOE II ultérieurement).

iLO 2, RILOE et RILOE II fonctionnent avec eDirectory uniquement dans le cadre de l'option HP Extended.

Consultez la liste complète des avantages disponibles dans la section « Avantages de l'intégration d'annuaire » (Avantages de l'intégration d'annuaire à la page 149). La section « Supervision distante activée via l'annuaire » (Supervision distante activée via l'annuaire à la page 184) explique en détail comment activer et appliquer les rôles, les groupes et la sécurité à l'aide des annuaires. Pour plus d'informations sur l'intégration d'annuaire, des livres blancs sont également disponibles sur le site Web HP (http://www.hp.com/servers/lights-out).

Avantages de l'intégration d'annuaire

- Évolutivité : l'annuaire peut être configuré pour prendre en charge des milliers d'utilisateurs sur des milliers de cartes iLO 2.
- Sécurité : des stratégies de mot de passe évoluées sont héritées de l'annuaire. La complexité, la fréquence de changement et l'expiration des mots de passe utilisateur sont des exemples de stratégie.
- Anonymat (manque) : dans certains environnements, les utilisateurs partagent des comptes Lights-Out, ce qui empêche de connaître l'auteur d'une opération mais pas le compte (ou rôle) utilisé.

- Administration basée sur les rôles : vous pouvez créer des rôles (par exemple, bureau, contrôle à distance de l'hôte, contrôle complet) et y associer des utilisateurs ou groupes. Toute modification apportée à un rôle s'applique à l'ensemble des utilisateurs et périphériques Lights-Out associés.
- Point unique d'administration : vous pouvez utiliser des outils d'administration natifs tels que MMC et ConsoleOne pour administrer les utilisateurs Lights-Out.
- Imminence : toute modification apportée à l'annuaire s'applique immédiatement aux processeurs Lights-Out associés. Cela évite d'écrire le script de ce processus.
- Élimination d'un autre mot de passe et nom d'utilisateur : vous pouvez utiliser des comptes utilisateur et des mots de passe existants dans l'annuaire sans qu'il soit nécessaire d'enregistrer ou de rappeler un nouveau jeu de données pour Lights-Out.
- Souplesse : vous pouvez créer un rôle unique pour un utilisateur unique sur une carte iLO 2 unique, ou créer un rôle unique pour plusieurs utilisateurs sur plusieurs cartes iLO, ou utiliser une combinaison de rôles adaptée aux besoins spécifiques de votre entreprise.
- Compatibilité : l'intégration d'annuaire Lights-Out s'applique aux produits iLO 2, RILOE et RILOE II. L'intégration prend en charge Active Directory et eDirectory.
- Normes : la prise en charge d'annuaire Lights-Out est basée sur la norme LDAP 2.0 pour un accès sécurisé aux annuaires.

Avantages et inconvénients d'annuaires sans schéma et d'annuaire de schéma HP

Les annuaires améliorent la sécurité, en permettant de gérer l'accès et les droits à partir d'un emplacement centralisé. Les annuaires proposent également une souplesse de configuration. Certaines pratiques de configuration d'annuaires fonctionnent mieux avec iLO 2 que d'autres. Avant de configurer iLO 2 pour des annuaires, vous devez décider si vous souhaitez utiliser l'annuaire sans schéma ou les méthodes d'intégration d'annuaire de schéma HP. Répondez aux questions suivantes pour vous aider à évaluer vos exigences d'intégration d'annuaire :

1. Pouvez-vous appliquer des extensions de schéma à votre annuaire ?
   - Non - Utilisez-vous Microsoft Active Directory ?
   - Non - L'intégration d'annuaire peut ne pas être adaptée à votre environnement. Envisagez de déployer un serveur d'annuaire d'évaluation afin d'évaluer les avantages de l'intégration d'annuaire.

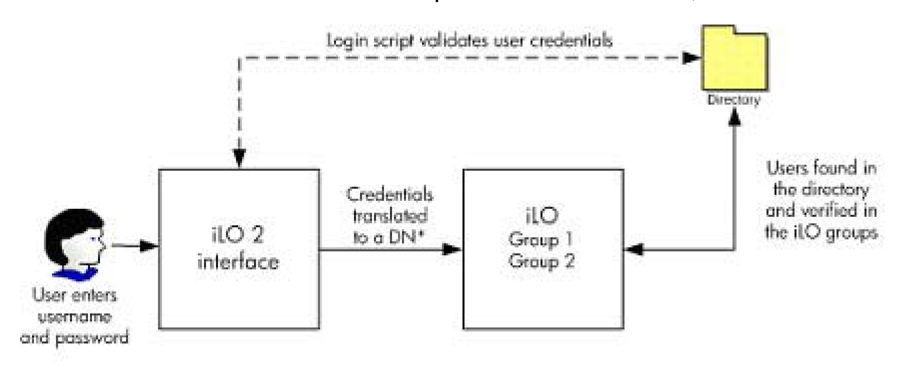
     — Oui - Utilisez une intégration d'annuaire sans schéma basée sur les groupes.
   - Oui - Passez à la question 2.
2. Votre configuration est-elle dimensionnable ?
   - Non - Déployez une instance de l'intégration d'annuaire sans schéma pour évaluer si la méthode d'intégration d'annuaire correspond à vos exigences de stratégie et de procédure. Si nécessaire, vous pouvez déployer une intégration d'annuaire de schéma HP ultérieurement.
   - Oui - Utilisez l'intégration d'annuaire de schéma HP.

     Les questions suivantes peuvent vous aider à déterminer si votre configuration est dimensionnable :
   - Envisagez-vous de modifier les droits ou privilèges d'un groupe d'utilisateurs d'annuaire ?

- Rédigerez-vous régulièrement des scripts de modification iLO 2 ?
- Utilisez-vous plus de cinq groupes pour contrôler les privilèges iLO 2 ?

Intégration d'annuaire sans schéma

Lors de l'utilisation de la méthode d'intégration d'annuaire sans schéma, les utilisateurs et appartenances aux groupes se trouvent dans l'annuaire, mais les privilèges de groupe se trouvent sur iLO 2. iLO 2 utilise les informations d'identification de connexion pour lire l'objet utilisateur dans l'annuaire et récupérer les appartenances aux groupes de l'utilisateur qui sont alors comparées à celles stockées dans iLO 2. Si une correspondance est trouvée, l'autorisation est accordée. Par exemple :



Avantages de l'utilisation de l'intégration d'annuaire sans schéma :

- Vous n'avez pas besoin d'étendre le schéma de l'annuaire.
- Lorsque les contrôles ActiveX sont activés dans le navigateur, la connexion à l'aide de NetBIOS et les formats d'e-mail sont pris en charge.
- Aucune ou peu de configuration n'est requis pour les utilisateurs dans l'annuaire. Si aucune configuration n'existe, l'annuaire exploite les utilisateurs et appartenances aux groupes existants pour accéder à iLO 2. Par exemple, si vous disposez d'un administrateur de domaine appelé Utilisateur1, vous pouvez copier le nom distinctif du groupe de sécurité de l'administrateur de domaine sur iLO 2 et lui accorder tous les privilèges. Utilisateur1 aura ensuite accès à iLO 2.

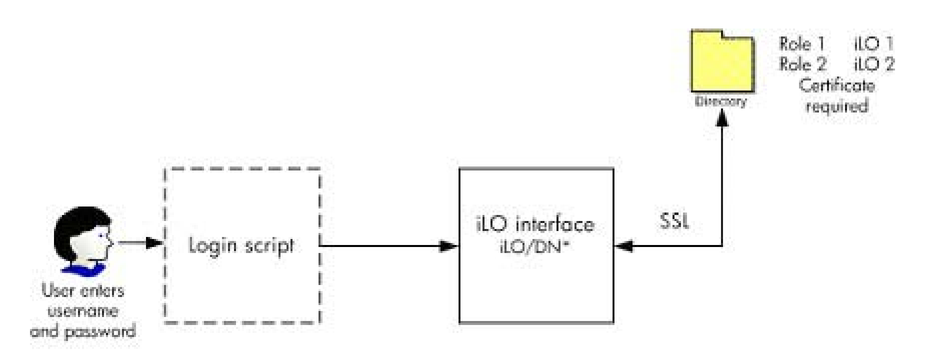
Inconvénients de l'utilisation de l'intégration d'annuaire sans schéma :

- Prend uniquement en charge Microsoft® Active Directory.
- Les privilèges de groupe sont administrés sur chaque iLO 2. Cependant, cet inconvénient est minimisé par le fait que les privilèges de groupe changent rarement. La modification des appartenances aux groupes est administrée dans l'annuaire et non sur chaque iLO 2. HP fournit des outils permettant de modifier simultanément un grand nombre d'iLO 2.

Intégration d'annuaire, dans le cadre du schéma HP

L'intégration d'annuaire de schéma HP est constituée d'une classe nommée hpqRole (une sous-classe de Group), une classe nommée hpqTarget (une sous-classe de User), ainsi que d'autres classes d'assistance. Une instance d'un hpqRole est simplement un rôle. Une instance d'un hpqTarget est équivalente à une carte iLO 2.

Un rôle contient une ou plusieurs cartes iLO 2 et un ou plusieurs utilisateurs, ainsi qu'une liste des privilèges dont disposent les utilisateurs avec la carte iLO 2 dans le rôle. Tous les accès iLO 2 sont gérés en ajoutant et supprimant des utilisateurs et cartes iLO 2 sur le rôle, et en supervisant les privilèges sur le rôle. Par exemple :



Avantages de l'utilisation de l'intégration d'annuaire de schéma HP :

- Plus grande souplesse de contrôle d'accès. Par exemple, vous pouvez limiter l'accès à une période de la journée, ou à partir d'une plage données d'adresses IP.
- Les groupes et les permissions sont conservés dans l'annuaire, non sur chaque iLO 2, et HP fournit les composants logiciels intégrables requis pour la supervision des cibles et groupes HP pour les utilisateurs et groupes Active Directory et pour eDirectory ConsoleOne.
- Intégration avec eDirectory

Inconvénients de l'intégration d'annuaire de schéma HP :

- Le schéma d'annuaire doit être étendu. Toutefois, cette tâche est minimisée car HP fournit le fichier .ldf et un assistant destiné à étendre le schéma, et les versions les plus récentes de Active Directory permettent d'annuler les modifications de schéma.

  Pour plus d'informations sur l'extension du schéma et de la configuration des informations de paramètres d'annuaire, reportez-vous à *Integrating HP ProLiant Lights-Out processors with Microsoft® Active Directory* (Intégration des processeurs HP ProLiant Lights-Out à l'aide de Microsoft® Active Directory) (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00190541/c00190541.pdf).
- Exigences de certificat

  iLO 2 doit communiquer avec l'annuaire en utilisant LDAP sur SSL. Cette communication requiert que le serveur d'annuaire dispose d'un certificat. L'installation du certificat pour le domaine le réplique dans l'ensembles des contrôleurs de domaine dans le domaine. Pour plus d'informations sur l'installation du certificat, reportez-vous à l'avis à la clientèle disponible sur le site Web HP (http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp).
- Options de basculement

  Pour activer le basculement (redondance), utilisez le nom de domaine en tant que nom de serveur d'annuaire lors de la configuration d'iLO 2. La plupart des serveurs DNS sont en mesure de résoudre un nom de domaine en serveur d'annuaire de travail (contrôleur de domaine).
- Format de connexion

  Les formats de noms NetBIOS, UPN et distinctifs sont acceptés comme noms de connexion. Le script de connexion pour iLO 2 communique avec le système d'exploitation client et tente de traduire le nom de connexion en un nom distinctif de l'annuaire. Pour que le script de connexion puisse réaliser cela, le nom d'annuaire doit être un nom DNS, et non une adresse IP. En outre, le client et la carte iLO 2 doivent pouvoir accéder au serveur d'annuaire en utilisant le même nom. Le client et la carte iLO 2 doivent être dans le même domaine DNS.
- Cibles multiples

Vous n'avez pas à utiliser des cibles multiples dans l'annuaire. L'intégration d'annuaire de schéma HP requiert uniquement un objet hpqTarget, qui peut représenter plusieurs périphériques LOM.

Configuration pour l'intégration d'annuaire sans schéma

Avant de configurer l'option sans schéma, votre système doit répondre à toutes les conditions requises décrites dans la section « Préparation d'Active Directory » (Préparation d'Active Directory à la page 153).

Vous pouvez configurer iLO 2 pour les annuaires de trois manières différentes :

- En utilisant manuellement un navigateur (Installation sans schéma basée sur le navigateur à la page 155).
- En utilisant un script (Installation sans schéma par script à la page 155).
- En utilisant HPLOMIG (Installation sans schéma basée sur HPLOMIG à la page 155).

Préparation d'Active Directory

L'option sans schéma est prise en charge sur les systèmes d'exploitation suivants :

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory

SSL doit être activé au niveau de l'annuaire. Pour activer SSL, installez un certificat pour le domaine dans Active Directory. iLO 2 communique avec l'annuaire uniquement via une connexion SSL sécurisée. Pour plus d'informations, reportez-vous à l'article 247078 de la Base de connaissances Microsoft® : *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers* (Activation des communications SSL via LDAP pour les contrôleurs de domaine Windows® 2000) sur le site Web Microsoft® (http://support.microsoft.com/).

Pour valider la configuration, vous devez avoir au minimum le nom distinctif dans l'annuaire d'un utilisateur et le nom distinctif d'un groupe de sécurité dont l'utilisateur est membre.

Introduction aux services de certificat

Les services de certificat permettent d'émettre des certificats numériques signés sur les hôtes du réseau. Les certificats permettent d'établir des connexions SSL avec l'hôte et de vérifier son authenticité.

L'installation des services de certificat permet à Active Directory de recevoir un certificat autorisant les processeurs Lights-Out à se connecter au service d'annuaire. Sans certificat, iLO 2 ne peut pas se connecter au serveur d'annuaire.

Chaque serveur d'annuaire auquel vous souhaitez que iLO 2 se connecte doit disposer d'un certificat. Si vous installez un service de certificat d'entreprise, Active Directory peut automatiquement demander et installer des certificats pour tous les contrôleurs Active Directory du réseau.

Installation des services de certificat

1. Sélectionnez **Démarrer>Paramètres>Panneau de configuration**.
2. Double-cliquez sur **Ajout/Suppression de programmes**.
3. Cliquez sur **Ajouter ou supprimer des composants Windows** pour lancer l'assistant Composants Windows.
4. Cochez la case **Services de certificat**. Cliquez sur **Suivant**.

5. Cliquez sur **OK** au message d'avertissement indiquant que le serveur ne peut pas être renommé. L'option Enterprise root CA (Autorité de certification d'entreprise) est sélectionnée car aucune autorité de certification n'est enregistrée dans Active Directory.
6. Entrez les informations appropriées pour votre site et votre organisation. Acceptez la période par défaut de deux ans pour le champ `Valid for` (Valide pendant). Cliquez sur **Suivant**.
7. Acceptez les emplacements par défaut de la base de données de certificats et du journal de base de données. Cliquez sur **Suivant**.
8. Accédez au dossier c:\I386 lorsque le système vous demande d'insérer le CD Windows® 2000 Advanced Server.
9. Cliquez sur **Terminer** pour fermer l'Assistant.

Vérification des services de certificat

Étant donné que les processeurs de supervision communiquent avec Active Directory via SSL, vous devez créer un certificat ou installer Certificate Services (Services de certificat). Vous devez installer une autorité de certification d'entreprise car vous enverrez des certificats aux objets dans votre domaine organisationnel.

Pour vérifier que des services de certification sont installés, sélectionnez **Démarrer>Programmes>Outils d'administration>Autorité de certification**. Si les services de certification ne sont pas installés, un message d'erreur s'affiche.

Configuration de demande de certificat automatique

Pour spécifier l'émission d'un certificat sur le serveur :

1. Sélectionnez **Démarrer>Exécuter**, puis entrez `mmc`.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Stratégie de groupe**, puis cliquez sur **Ajouter** pour ajouter le composant logiciel intégrable dans MMC.
4. Cliquez sur **Parcourir**, puis sélectionnez l'objet Default Domain Policy (Stratégie de domaine par défaut). Cliquez sur **OK**.
5. Sélectionnez **Terminer>Fermer>OK**.
6. Sélectionnez **Configuration ordinateur>Paramètres Windows>Paramètres de sécurité>Stratégies de clé publique**.
7. Cliquez avec le bouton droit sur **Automatic Certificate Requests Settings** (Paramètres de demande de certificat automatique), puis sélectionnez **New>Automatic Certificate Request** (Nouveau>Demande de certificat automatique).
8. Cliquez sur **Suivant** lorsque l'assistant Automatic Certificate Request Setup (Configuration de demande de certificat automatique) démarre.
9. Sélectionnez le modèle **Domain Controller** (Contrôleur de domaine), puis cliquez sur **Suivant**.
10. Sélectionnez l'autorité de certification listée. (Il s'agit de la même que celle définie lors de l'installation des services de certificat). Cliquez sur **Suivant**.
11. Cliquez sur **Terminer** pour fermer l'Assistant.

Installation sans schéma basée sur le navigateur

L'installation sans schéma peut se faire via l'interface iLO 2 basée sur le navigateur.

1. Connectez-vous à la carte iLO 2 en utilisant un compte doté du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2). Cliquez sur **Administration**.

   REMARQUE : seuls les utilisateurs dotés du privilège Configure iLO 2 Settings (Configurer paramètres iLO 2) sont autorisés à modifier ces paramètres. Les autres peuvent uniquement consulter les paramètres attribués.

2. Cliquez sur **Directory Settings** (Paramètres d'annuaire).
3. Sélectionnez **Use Directory Default Schema** (Utiliser le schéma d'annuaire par défaut) dans la section Authentication Settings (Paramètres d'authentification). Pour plus d'informations, reportez-vous à la section « Options d'installation sans schéma » (Options de l'installation sans schéma à la page 155).
4. Cliquez sur **Apply Settings** (Appliquer les paramètres).
5. Cliquez sur **Test Settings** (Tester paramètres).

Installation sans schéma par script

Pour installer l'option d'annuaires sans schéma à l'aide de la rédaction de scripts XMS RIBCL :

1. Téléchargez et consultez le manuel des ressources de la ligne de commande et des scripts.
2. Rédigez un script qui configure iLO 2 pour la prise en charge d'annuaires sans schéma, puis exécutez-le. Le script suivant peut servir de modèle.

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="admin" PASSWORD="password">
<DIR_INFO MODE = "write">
<MOD_DIR_CONFIG>
<DIR_ENABLE_GRP_ACCT value = "yes"/>
<DIR_GRPACCT1_NAME value ="CN=Administrators,
CN=Builtin,DC=HP,DC=com "/>
<DIR_GRPACCT1_PRIV value = "1"/>
</MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>
```

Installation sans schéma basée sur HPLOMIG

HPLOMIG est la méthode la plus simple pour installer un grand nombre de processeurs LOM pour des annuaires. Pour utiliser HPLOMIG, téléchargez l'utilitaire du même nom et la documentation qui l'accompagne via le site Web HP (http://www.hp.com/servers/lights-out). HP recommande l'utilisation de HPLOMIG lorsque vous configurez de nombreux processeurs LOM pour des annuaires. Pour plus d'informations sur l'emploi de l'utilitaire HPLOMIG, reportez-vous à la section « Utilitaire de migration d'annuaire HPQLOMIG » (Utilitaire de migration d'annuaire HPQLOMIG à la page 192).

Options de l'installation sans schéma

Les options d'installation sont les mêmes, quelle que soit la méthode (navigateur, HPQLOMIG ou script) que vous utilisez pour configurer l'annuaire.

Après avoir activé les annuaires et sélectionné l'option sans schéma, vous avez les possibilités suivantes :

Souplesse d'ouverture de session minimale

- Saisissez le nom DNS ou l'adresse IP et le port LDAP du serveur d'annuaire. Généralement, le port LDAP pour une connexion SSL est 636.
- Saisissez le nom distinctif d'un groupe au moins. Il peut s'agir d'un groupe de sécurité (par exemple : « CN=Administrators,CN=Builtin,DC=HP,DC=com ») ou tout autre groupe, à condition que les utilisateurs iLO 2 qui font l'objet de l'installation en soient membres.

  Avec une configuration minimale, vous pouvez vous connecter à iLO 2 à l'aide de votre distinctif complet et de votre mot de passe. Vous devez être membre d'un groupe reconnu par iLO 2.

Souplesse d'ouverture de session améliorée

- Outre les paramètres minimaux, indiquez au moins un contexte utilisateur d'annuaire.

  Au moment de l'ouverture de session, le nom de connexion et le mot de passe sont combinés pour former le nom distinctif de l'utilisateur. Par exemple, si l'utilisateur se connecte en tant que « JOHN.SMITH » et qu'un contexte utilisateur est défini en tant que « CN=USERS,DC=HP,DC=COM », le nom distinctif qui sera utilisé par iLO 2 sera « CN=JOHN.SMITH,CN=USERS,DC=HP,DC=COM ».

Souplesse d'ouverture de session maximale

- Configurez iLO 2 conformément à la description.
- Configurez iLO 2 avec un nom de DNS et non une adresse IP pour l'adresse réseau du serveur d'annuaire. Le nom de DNS doit être résolvable en adresse IP à la fois à partir d'iLO 2 et du système client.
- Activez les contrôles ActiveX dans votre navigateur. Le script de connexion iLO 2 va tenter d'appeler un contrôle Windows® pour convertir le nom de connexion en nom distinctif.

  La configuration d'iLO 2 avec le niveau maximum de souplesse d'ouverture de session vous permet de vous connecter avec votre nom distinctif complet et votre mot de passe, votre nom tel qu'il apparaît dans l'annuaire, le format NetBIOS (domaine/nom_connexion) ou le format d'e-mail (nom_connexion@domaine).

REMARQUE : vos paramètres de sécurité du système ou vos logiciels installés peuvent empêcher le script de connexion d'appeler le contrôle ActiveX Windows®. Dans ce cas, votre navigateur affiche un message d'avertissement dans la barre d'état ou une zone de message, ou bien il cesse de répondre. Pour essayer d'identifier le logiciel ou paramètre à l'origine du problème, créez un autre profil et connectez-vous au système.

Dans certains cas, il est possible que vous ne puissiez pas faire fonctionner l'option de souplesse d'ouverture de session maximale. Par exemple, si le client et iLO 2 se trouvent dans des domaines DNS différents, il peut arriver que l'un des deux soit dans l'impossibilité de résoudre le nom du serveur d'annuaire en adresse IP.

Groupes imbriqués sans schéma

De nombreuses organisations répartissent les utilisateurs et administrateurs en groupes. Disposer de cette organisation de groupes existants est pratique car vous pouvez les associer à un ou plusieurs objets de rôle Integrated Lights-Out Management. Lorsque les périphériques sont associés à des objets de rôle, l'administrateur contrôle l'accès aux périphériques Lights-Out associés au rôle en ajoutant ou supprimant des membres au sein des groupes.

Lors de l'utilisation de Microsoft® Active Directory, vous pouvez placer un groupe au sein d'un autre, en créant ainsi un groupe imbriqué. Les objets de rôle sont considérés comme des groupes et peuvent en inclure d'autres directement. Vous pouvez ajouter directement le groupe imbriqué existant au rôle et affecter les privilèges et les restrictions appropriés. De nouveaux utilisateurs peuvent venir s'ajouter au groupe existant ou au rôle.

Dans les mises en œuvre précédentes, seul un utilisateur sans schéma, qui était membre direct du groupe principal, était autorisé à se connecter à iLO 2. En utilisant l'intégration sans schéma, les utilisateurs qui sont des membres indirects (un membre d'un groupe appartenant au groupe principal) sont autorisés à se connecter à iLO 2.

Novell eDirectory n'autorise pas l'imbrication des groupes. Dans eDirectory, tout utilisateur pouvant lire un rôle est considéré comme l'un de ses membres. Lors de l'ajout d'un groupe existant, d'une unité organisationnelle ou d'une organisation à un rôle, ajoutez l'objet en tant qu'administrateur en lecture de ce rôle. Tous les membres de cet objet sont considérés comme membres de ce rôle. Il est possible d'ajouter de nouveaux utilisateurs au groupe existant ou au rôle.

Lors de l'utilisation d'affectations de privilèges d'annuaire ou administrateur dans le but d'augmenter le nombre des membres du rôle, les utilisateurs doivent pouvoir lire l'objet LOM correspondant au périphérique LOM. Certains environnements requièrent que les administrateurs d'un rôle soient également administrateurs en lecture de l'objet LOM afin d'authentifier correctement les utilisateurs.

Configuration de l'intégration d'annuaire dans le cadre du schéma HP

Lorsque vous utilisez l'intégration d'annuaire dans le cadre du schéma HP, iLO 2 prend en charge à la fois Active Directory et eDirectory. Toutefois, ces services d'annuaire requièrent une extension du schéma.

Fonctionnalités prises en charge par l'intégration d'annuaire dans le cadre du schéma HP

La fonctionnalité iLO 2 Directory Services (Services d'annuaire iLO 2) permet d'effectuer les tâches suivantes :

- authentifier des utilisateurs à partir d'une base de données utilisateur évolutive, consolidée et partagée ;
- contrôler les privilèges utilisateur (autorisation) à l'aide du service d'annuaire ;
- utiliser des rôles dans le service d'annuaire pour l'administration au niveau du groupe des processeurs de supervision iLO 2 et des utilisateurs iLO 2.

Cette opération doit être effectuée par un administrateur de schéma. La base de données des utilisateurs locaux est conservée. Le client peut choisir de ne pas utiliser d'annuaire, de recourir à une combinaison d'annuaires et de comptes locaux ou de faire appel à des annuaires exclusivement pour l'authentification.

REMARQUE : lorsque vous vous connectez via Diagnostics Port (Port de diagnostics), le serveur d'annuaire n'est pas disponible. Vous pouvez uniquement ouvrir une session à l'aide d'un compte local.

Configuration des services d'annuaire

Pour activer correctement la supervision via l'annuaire sur n'importe quel processeur de supervision Lights-Out :

1. Planification

Passez en revue les sections suivantes :

- « Services d'annuaire » (Services d'annuaire à la page 149)
- « Schéma des services d'annuaire » (Schéma des services d'annuaire à la page 238)
- « Supervision distante activée via l'annuaire » (Supervision distante activée via l'annuaire à la page 184)

2. Installation

   a. Téléchargez la solution HP Lights-Out Directory Package contenant le programme d'installation de schémas, le programme d'installation de composants logiciels intégrables de supervision et les utilitaires de migration depuis le site Web HP (http://www.hp.com/servers/lights-out).

   b. Exécutez une fois le programme d'installation de schémas (Programme d'installation de schémas à la page 160) pour étendre le schéma.

   c. Exécutez le programme d'installation de composants logiciels intégrables de supervision (Programme d'installation de composants logiciels intégrables de supervision à la page 162) et installez le composant logiciel intégrable approprié à votre service d'annuaire sur une ou plusieurs stations de supervision.

3. Mise à jour

   a. Flashez la ROM sur le processeur de supervision Lights-Out avec le microprogramme activé par l'annuaire.

   b. Réglez les paramètres serveur et le nom distinctif des objets du processeur de supervision sur la page Directory Settings (Directory Settings (Paramètres d'annuaire) à la page 52) (Paramètres d'annuaire) dans l'interface graphique iLO 2.

4. Supervision

   a. Créez un objet de périphérique de supervision et un objet de rôle (Objets de services d'annuaire à la page 169) à l'aide du composant logiciel intégrable.

   b. Affectez des droits à l'objet de rôle, selon les besoins, et associez le rôle à l'objet de périphérique de supervision.

   c. Ajoutez des utilisateurs aux objets de rôle.

      Pour plus d'informations sur la supervision du service d'annuaire, reportez-vous à la section « Supervision distante activée via l'annuaire » (Supervision distante activée via l'annuaire à la page 184). Vous trouverez des exemples dans les sections « Services d'annuaire pour Active Directory » (Services d'annuaire pour Active Directory à la page 162) et « Services d'annuaire pour eDirectory » (Services d'annuaire pour eDirectory à la page 173).

5. Gestion des exceptions

   - Les utilitaires de migration Lights-Out sont plus faciles à utiliser avec un rôle Lights-Out unique. Si vous prévoyez de créer plusieurs rôles dans l'annuaire, il peut s'avérer nécessaire d'utiliser des utilitaires de génération de scripts d'annuaire tels que le script LDIFDE ou VB pour créer des combinaisons de rôles complexes. Pour plus d'informations, reportez-vous à la section « Utilisation des outils d'importation en masse » (Utilisation des outils d'importation en masse à la page 190).
   - Si votre ancien microprogramme est doté de processeurs iLO 2 ou RILOE, il peut s'avérer nécessaire de le mettre à jour manuellement à l'aide d'un navigateur. La configuration minimale requise pour mettre à jour le microprogramme à distance à l'aide des scripts RIBCL et de l'utilitaire de migration d'annuaire est la suivante :

Produit LOM	Version minimale du microprogramme
RILOE	2.41
RILOE II	Toutes versions
iLO	1.4x
iLO 2	1.1x

Une fois le schéma étendu, vous pouvez procéder à la configuration des services d'annuaire à l'aide des utilitaires de migration des annuaires HP Lights-Out (Utilitaire de migration d'annuaire HPQLOMIG à la page 192). Les utilitaires de migration sont inclus dans la solution HP Lights-Out Directory Package. La version 1.13 de l'utilitaire de migration d'annuaire permet à Lights-Out d'importer et d'exporter, et prend en charge les diverses données utilisateur pour chaque processeur Lights-Out.

Documentation sur les schémas

Pour vous aider dans le processus de planification et d'approbation, HP fournit de la documentation sur les modifications apportées au schéma au cours de la procédure de configuration de ce dernier. Pour passer en revue les modifications apportées au schéma existant, reportez-vous à la section « Schéma des services d'annuaire » (Schéma des services d'annuaire à la page 238).

Prise en charge des services d'annuaire

Avec l'intégration d'annuaire dans le cadre du schéma HP, iLO 2 prend en charge les services d'annuaire suivants :

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory
- Microsoft® Windows® Server 2008 Active Directory
- Novell eDirectory 8.7.3
- Novell eDirectory 8.7.1

Le logiciel iLO 2 est conçu pour être utilisé avec les outils de supervision Microsoft® Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory) et Novell ConsoleOne, ce qui permet de superviser des comptes utilisateur sur Microsoft Active Directory ou Novell eDirectory. Cette solution ne fait aucune distinction entre les services eDirectory utilisés sur NetWare, Linux ou Windows®. L'extension du schéma de eDirectory requiert la version 1.4.0 ou ultérieure de la Machine virtuelle Java™ pour l'authentification SSL.

La carte iLO 2 prend en charge l'utilisation de Microsoft® Active Directory sur les systèmes d'exploitation suivants :

- Windows Server® 2008
- Windows Server® 2003

iLO 2 utilise le logiciel Novell pour prendre en charge eDirectory.

Logiciels requis pour les schémas

La carte iLO 2 requiert des logiciels spécifiques pour étendre le schéma et fournir des composants logiciels intégrables permettant de superviser votre réseau iLO 2. Un composant HP Smart téléchargeable contient le programme d'installation de schémas et de composants logiciels intégrables de supervision. Il est téléchargeable à partir du site Web HP (http://www.hp.com/servers/lights-out).

Le programme d'installation de schémas ne peut être installé sur un contrôleur de domaine hébergeant Windows Server® 2008 Core. Pour des raisons de sécurité et de performance, Windows Server® 2008 Core n'utilise pas d'interface utilisateur graphique. Pour utiliser le programme d'installation de schémas, vous devez installer une interface utilisateur graphique, ou utiliser un contrôleur de domaine hébergeant une version plus récente de Windows®.

Programme d'installation de schémas

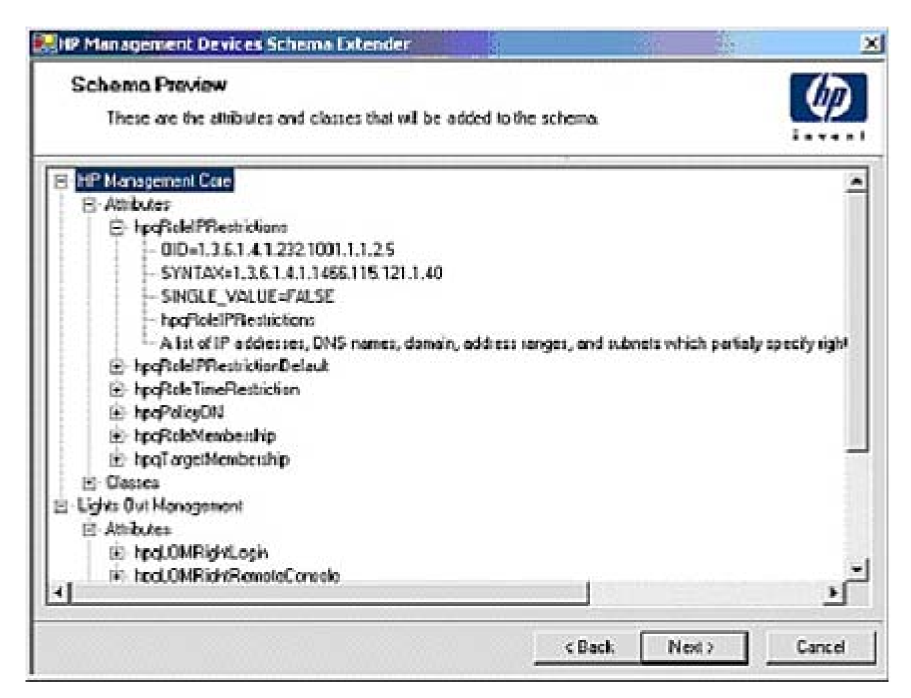
Le programme d'installation de schémas est fourni avec un ou plusieurs fichiers .xml. Ces fichiers contiennent le schéma à ajouter à l'annuaire. En général, un des fichiers contient le schéma central commun à tous les services d'annuaire pris en charge. Les autres contiennent uniquement des schémas propres au produit. .NET Framework est obligatoire pour utiliser le programme d'installation.

Le programme d'installation comporte trois écrans importants :

- Schema Preview (Aperçu du schéma)
- Configuration
- Results (Résultats)

Schema Preview (Aperçu du schéma)

L'écran Schema Preview (Aperçu du schéma) permet à l'utilisateur de visualiser les extensions proposées du schéma. Cet écran lit les fichiers de schéma sélectionnés, analyse le code XML et l'affiche sous la forme d'une arborescence. Il répertorie tous les détails des attributs et des classes qui seront installés.



Configuration

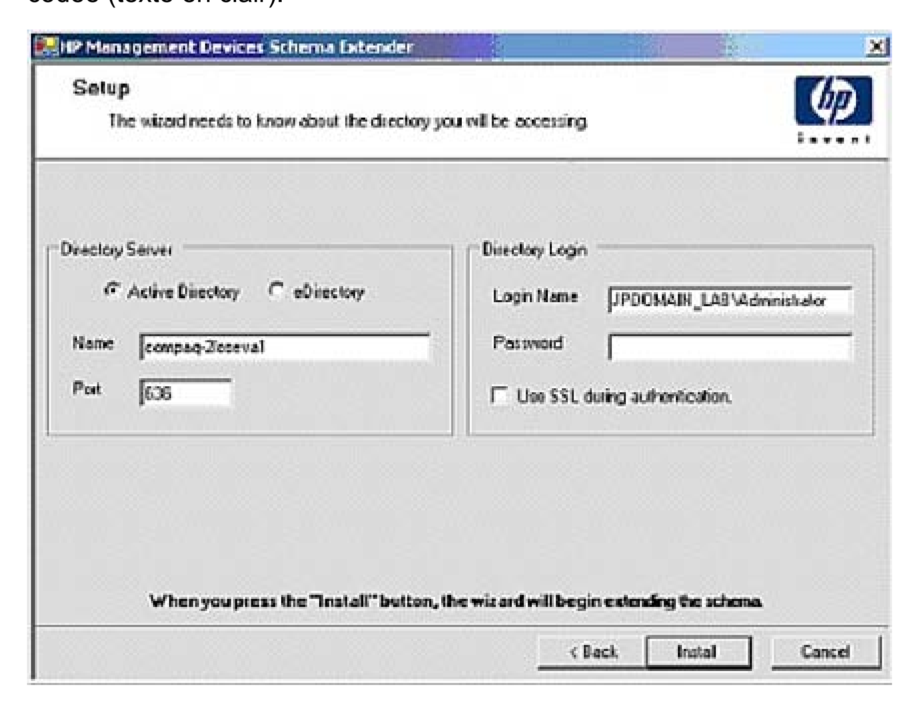
L'écran Setup (Configuration) permet d'entrer les informations pertinentes avant l'extension du schéma.

La section Directory Server (Serveur d'annuaire) de l'écran Setup (Configuration) permet de sélectionner Active Directory ou eDirectory et de paramétrer le nom de l'ordinateur et le port à utiliser pour les communications LDAP.

REMARQUE : pour pouvoir étendre le schéma sur Active Directory, il faut que l'utilisateur soit un administrateur de schémas authentifié, que le schéma ne soit pas protégé en écriture et que l'annuaire soit propriétaire du rôle FSMO dans l'arborescence. Le programme d'installation tâchera de faire du serveur d'annuaire cible le contrôleur de schéma FSMO de la forêt.

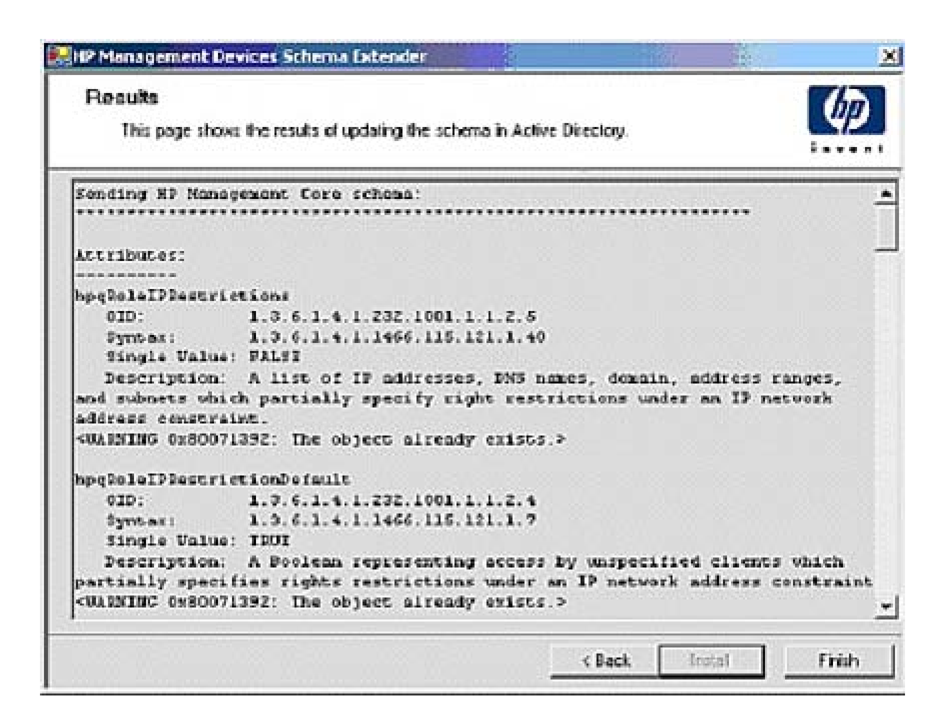
Pour obtenir un accès en écriture au schéma sur Windows® 2000, il convient de modifier le verrouillage de sécurité du registre. Si l'utilisateur sélectionne l'option **Active Directory**, le composant d'extension de schéma essaiera d'effectuer cette modification. Pour que cette opération aboutisse, l'utilisateur doit obligatoirement disposer des droits appropriés. L'accès en écriture au schéma est automatiquement activé sur Windows® Server 2003.

La section Directory Login (Connexion à l'annuaire) de l'écran Setup (Configuration) vous permet d'entrer votre nom de connexion et votre mot de passe. Ils peuvent s'avérer nécessaires pour procéder à l'extension du schéma. L'option Use SSL during authentication (Utiliser SSL pendant authentification) détermine le type d'authentification sécurisée à utiliser. Si cette option est sélectionnée, le protocole SSL permet d'authentifier l'annuaire. Si elle ne l'est pas et que la fonction Active Directory l'est, c'est l'authentification Windows NT® qui est utilisée. Si elle ne l'est pas et que la fonction eDirectory l'est, l'authentification de l'administrateur et l'extension du schéma s'effectuent à l'aide d'une connexion non codée (texte en clair).



Results (Résultats)

L'écran Results (Résultats) affiche les résultats de l'installation, notamment si le schéma a été étendu et les attributs qui ont été modifiés.



Programme d'installation de composants logiciels intégrables de supervision

Le programme d'installation de composants logiciels intégrables de supervision installe les composants nécessaires pour superviser les objets iLO 2 dans l'annuaire Microsoft® Active Directory Users and Computers (Utilisateurs et ordinateurs) ou Novell ConsoleOne.

Les composants logiciels intégrables iLO 2 sont utilisés pour exécuter les tâches suivantes lors de la création d'un annuaire iLO 2 :

- création et supervision des objets iLO 2 et des objets de rôle (les objets de stratégie seront pris en charge ultérieurement) ;
- création d'associations entre les objets iLO 2 et les objets de rôle (ou de stratégie).

Services d'annuaire pour Active Directory

Les sections suivantes décrivent les conditions préalables à l'installation des services d'annuaire pour Active Directory, ainsi que les procédures de préparation et un exemple pratique. HP fournit un utilitaire permettant d'automatiser un grand nombre de processus de configuration d'annuaire. Vous pouvez télécharger la prise en charge des annuaires HP pour les processeurs de supervision sur le site Web HP (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

Conditions préalables à l'installation de Active Directory

- Active Directory doit disposer d'un certificat numérique pour permettre à iLO 2 de se connecter sur le réseau en toute sécurité.
- Active Directory doit disposer du schéma étendu pour décrire les propriétés et classes d'objet Lights-Out.
- La version du microprogramme doit être iLO v1.40 ou version ultérieure, ou iLO v1.00 ou version ultérieure.
- Vous devez disposer d'une licence pour les fonctions avancées de iLO 2.

Vous pouvez évaluer iLO Advanced avec une clé de licence d'évaluation gratuite téléchargeable à partir du site Web HP (http://h10018.www1.hp.com/wwsolutions/ilo/iloeval.html).

Les services d'annuaire de la carte iLO 2 utilisent le protocole LDAP sur SSL pour communiquer avec les serveurs d'annuaire. Avant d'installer les composants logiciels intégrables et le schéma correspondant à Active Directory, lisez et gardez à disposition la documentation suivante :

REMARQUE : l'installation de la fonction Directory Services (Services d'annuaire) pour la carte iLO 2 requiert l'extension du schéma de Active Directory. Cette extension doit être réalisée par un administrateur de schémas Active Directory.

- *Extending the Schema* (Extension du schéma) dans le kit Microsoft® Windows® 2000 Server Resource Kit, disponible sur le site Web Microsoft® (http://msdn.microsoft.com).
- *Installing Active Directory* (Installation de Active Directory) dans le kit Microsoft® Windows® 2000 Server Resource Kit.
- Articles de la base de connaissances Microsoft®.

  Ces articles sont accessibles à l'aide de l'option Knowledge Base Article ID Number Search (Recherche de numéro d'ID d'article de la base de connaissances) disponible sur le site Web Microsoft® (http://support.microsoft.com/).

  - 216999 *Installing the Remote Server Administration Tools in Windows® 2000 (Installation des outils d'administration du serveur distant sous Windows® 2000)*
  - 314978 *Using the Adminpak.msi to Install a Server Administration Tool in Windows® 2000 (Utilisation de Adminpak.msi pour installer un outil d'administration du serveur sous Windows® 2000)*
  - 247078 *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers (Activation de la communication SSL sur LDAP pour les contrôleurs de domaine Windows® 2000)*
  - 321051 *Enabling LDAP over SSL with a Third-Party Certificate Authority (Activation de LDAP sur SSL par une autorité de certification tierce)*
  - 299687 *MS01-036 : Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed (La fonction concernée par l'utilisation du protocole LDAP via SSL peut activer les mots de passe à modifier)*

La carte iLO 2 nécessite une connexion sécurisée pour communiquer avec le service d'annuaire. Ceci requiert l'installation de Microsoft® CA. Reportez-vous à l'article 321051 de la base de connaissances de références techniques Microsoft® : *How to Enable LDAP over SSL with a Third-Party Certification Authority* (Activation du protocole LDAP sur SSL avec une autorité de certification tierce).

Installation de Active Directory sur Windows Server 2008

Pour le schéma par défaut :

1. Désactivez IPV6, puis installez Active Directory, DNS et l'autorité de certification racine dans Windows Server® 2008.
2. Connectez-vous à iLO, puis accédez à la page Directory Settings (Paramètres d'annuaire). Cliquez sur **Administration>Security>Directory** (Administration>Sécurité>Annuaire).
3. Dans Directory Settings (Paramètres d'annuaire), entrez les paramètres de votre annuaire.
4. Dans le contexte d'utilisateur d'annuaire, entrez les paramètres de votre annuaire.

5. Créez les Administer Groups (Administrer les groupes) pour vos utilisateurs iLO.
6. Cliquez sur **Administration>Network>DHCP/DNS** (Administration>Réseau>DHCP/DNS). Modifiez ensuite les paramètres de votre environnement dans Domain Name (Nom de domaine) et dans Primary DNS server, (Serveur DNS principal).

Pour le schéma étendu :

1. Désactivez IPV6, puis installez Active Directory, DNS et l'autorité de certification racine dans Windows Server® 2008.
2. Le composant LDAP de iLO requiert l'installation de .Net Framework 1.1_4322. Installez .Net Framework.
3. Installez le dernier composant LDAP de iLO (version sp31581 ou ultérieure).
4. Étendez le schéma à l'aide de l'utilitaire d'extension des périphériques de supervision HP.
5. Installez le composant LDAP intégrable de HP.
6. Créez le périphérique HP, ainsi que le rôle HP.
7. Connectez-vous à iLO, puis accédez à la page Directory Settings (Paramètres d'annuaire). Cliquez sur **Administration>Security>Directory** (Administration>Sécurité>Annuaire).
8. Entrez les paramètres d'annuaire pour votre annuaire.
9. Entrez le contexte d'utilisateur d'annuaire.
10. Cliquez sur **Administration>Network>DHCP/DNS** (Administration>Réseau>DHCP/DNS). Modifiez ensuite les paramètres de votre environnement dans Domain Name (Nom de domaine) et dans Primary DNS server (Serveur DNS principal).

Le composant LDAP ne fonctionne pas avec une installation centrale (« core ») de Windows Server® 2008.

Préparation des services d'annuaire pour Active Directory

Pour configurer les services d'annuaire afin de les utiliser avec les processeurs de supervision iLO 2, procédez comme suit :

1. Installez Active Directory. Pour plus d'informations, reportez-vous au document *Installing Active Directory* (Installation de Active Directory) disponible dans le kit de ressources de Microsoft® Windows® 2000 Server.
2. Installez le Microsoft® Admin Pack (le fichier ADMINPAK.MSI, situé dans le sous-répertoire i386 du CD Windows® 2000 Server ou Advance Server). Pour plus d'informations, reportez-vous à l'article 216999 de la Base de connaissances Microsoft®.
3. Dans Windows® 2000, le verrouillage de sécurité qui empêche toute écriture accidentelle sur le schéma doit être temporairement désactivé. L'utilitaire d'extension du schéma permet de le faire si le service de registre distant est exécuté et que l'utilisateur dispose des privilèges appropriés. Vous pouvez également paramétrer `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ServicesParameters\Schema Update Allowed` dans le registre sur une valeur autre que zéro (reportez-vous à la section « Déroulement du traitement lors de l'extension du schéma » du fichier *Installation of Schema Extensions* [Installation des extensions de schéma] du kit Windows® 2000 Server Resource Kit) ou exécuter la procédure suivante. Cette étape n'est pas nécessaire sous Windows® 2003 Server.

REMARQUE : la modification incorrecte du registre peut gravement endommager votre système. HP vous recommande de créer une copie de sauvegarde de toutes les données importantes contenues sur l'ordinateur avant de modifier le registre.

a. Démarrez MMC.

b. Installez le composant logiciel intégrable Active Directory Schema (Schéma Active Directory) dans MMC.

c. Cliquez avec le bouton droit sur **Active Directory Schema**(Schéma Active Directory) et sélectionnez **Operations Master** (Maître des opérations).

d. Sélectionnez **The Schema may be modified on this Domain Controller** (Le schéma peut être modifié sur ce contrôleur de domaine).

e. Cliquez sur **OK**.

Il peut s'avérer nécessaire de développer le dossier Active Directory Schema (Schéma Active Directory) pour que la case à cocher apparaisse.

4. Créez un certificat ou installez Certificate Services (Services de certificat). Cette étape est nécessaire pour créer un certificat ou installer Certificate Services (Services de certificat) dans la mesure où la carte iLO 2 communique avec Active Directory à l'aide de SSL. Vous devez installer Active Directory avant Certificate Services (Services de certificat).

5. Pour spécifier l'émission d'un certificat sur le serveur qui exécute Active Directory :

a. Lancez Microsoft® Management Console (Console de supervision Microsoft) sur le serveur et ajoutez le composant logiciel intégrable de stratégie du domaine par défaut (Group Policy - Stratégie de groupe), puis naviguez jusqu'à Default domain policy object (Objet de stratégie du domaine par défaut).

b. Cliquez sur **Configuration ordinateur>Paramètres Windows>Paramètres de sécurité>Stratégies de clé publique**.

c. Cliquez avec le bouton droit sur **Automatic Certificate Requests Settings** (Paramètres de demande de certificat automatique), puis sélectionnez **New>Automatic Certificate Request** (Nouveau>Demande de certificat automatique).

d. Utilisez l'assistant pour sélectionner le modèle de contrôleur de domaine et l'autorité de certification de votre choix.

6. Téléchargez le composant Smart qui contient les programmes d'installation relatifs à l'utilitaire d'extension de schéma et aux composants logiciels intégrables. Le composant Smart est téléchargeable à partir du site Web HP (http://www.hp.com/servers/lights-out).

7. Exécutez le programme d'installation de schéma pour étendre le schéma. Ce programme ajoute les objets HP appropriés au schéma.

Le programme d'installation de schémas associe les composants logiciels intégrables Active Directory au nouveau schéma. L'utilitaire de configuration de l'installation des composants logiciels intégrables est un script de configuration Windows MSI qui est exécuté partout où MSI est pris en charge (Windows® XP, Windows® 2000, Windows® 98). Certaines parties de l'application d'extension du schéma ont toutefois besoin de .NET Framework, téléchargeable sur le site Web Microsoft® (http://www.microsoft.com).

Installation et initialisation des composants logiciels intégrables pour Active Directory

1. Exécutez l'application d'installation des composants logiciels intégrables.
2. Configurez le service d'annuaire de manière à disposer des objets et des relations appropriés pour la supervision de la carte iLO 2.
    a. Utilisez les composants logiciels intégrables de supervision de HP pour créer des objets iLO 2, de stratégie et de rôle administrateur et utilisateur.
    b. Utilisez les composants logiciels intégrables de supervision de HP pour créer des associations entre l'objet iLO 2, l'objet de stratégie et l'objet de rôle.
    c. Reliez l'objet iLO 2 aux objets de rôle administrateur et utilisateur (les rôles administrateur et utilisateur renvoient automatiquement à l'objet iLO 2).

    Pour plus d'informations concernant les objets iLO 2, reportez-vous à la section « Objets de services d'annuaire » (Objets de services d'annuaire à la page 169).

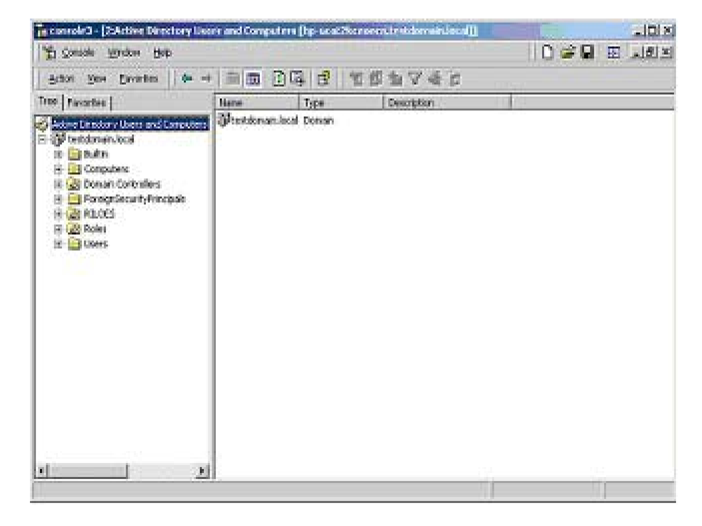
Vous devez au minimum créer :

- un objet de rôle contenant un ou plusieurs utilisateurs et un ou plusieurs objets iLO 2 ;
- un objet iLO 2 correspondant à chaque processeur de supervision iLO 2 qui utilisera l'annuaire.

Exemple : création et configuration d'objets d'annuaire destinés à être utilisés avec la carte iLO 2 dans Active Directory

L'exemple suivant montre comment définir des rôles et des périphériques HP dans l'annuaire d'une entreprise à l'aide du domaine *testdomain.local*, qui se compose de deux unités organisationnelles, *Roles* et *RILOES*.

Imaginons qu'une société possède un annuaire d'entreprise incluant le domaine *testdomain.local*, organisé comme illustré dans l'écran suivant.



Créez une unité organisationnelle qui contiendra les périphériques Lights-Out supervisés par le domaine. Dans cet exemple, deux unités organisationnelles sont créées : *Roles* et *RILOES*.

1. Utilisez les composants logiciels intégrables Active Directory Users and Computers (Utilisateurs et ordinateurs) fournis par HP pour créer des objets de supervision Lights-Out dans l'unité organisationnelle *RILOES* pour plusieurs périphériques iLO 2.

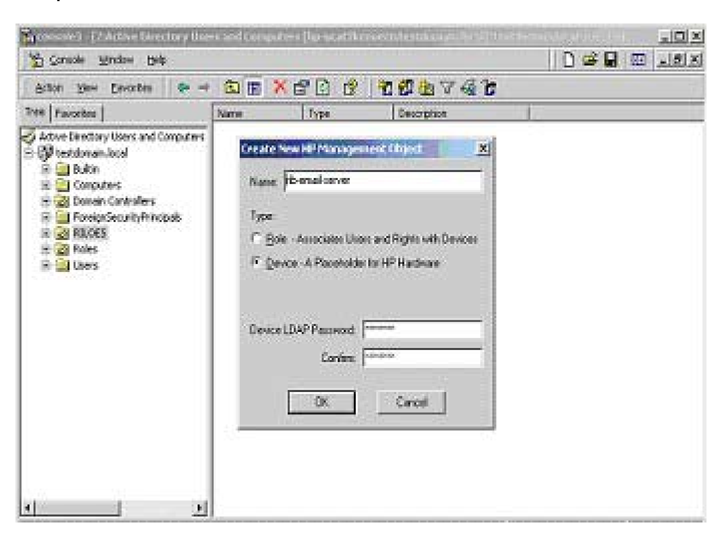
   a. Cliquez avec le bouton droit sur l'unité organisationnelle RILOES localisée dans le domaine *testdomain.local* et sélectionnez **NewHPObject** (Nouvel objet HP).

   b. Sélectionnez **Device** (Périphérique) dans la boîte de dialogue Create New HP Management Object (Créer nouvel objet de supervision HP).

   c. Entrez un nom approprié dans le champ Name (Nom) de la boîte de dialogue. Dans cet exemple, le nom d'hôte DNS du périphérique iLO 2, *rib-email-server*, est utilisé comme nom de l'objet de supervision Lights-Out, tandis que le nom de famille est *RILOEII*.

      Entrez et confirmez le mot de passe dans les champs Device LDAP Password (Mot de passe LDAP du périphérique) et Confirm (Confirmation). Le périphérique utilise ce mot de passe pour authentifier l'annuaire, il doit donc être unique. Ce mot de passe est celui utilisé dans l'écran Directory Settings (Paramètres d'annuaire) de la carte iLO 2.

   d. Cliquez sur **OK**.



2. Utilisez les composants logiciels intégrables Active Directory Users and Computers (Utilisateurs et ordinateurs) fournis par HP pour créer des objets de rôle HP dans l'unité organisationnelle *Roles*.

   a. Cliquez avec le bouton droit sur l'unité organisationnelle Roles, puis sélectionnez **New** (Nouveau), puis **Object** (Objet).

   b. Sélectionnez **Role** (Rôle) dans le champ Type de la boîte de dialogue Create New HP Management Object (Créer nouvel objet de supervision HP).

   c. Entrez un nom approprié dans le champ Name (Nom) de la boîte de dialogue New HP Management Object (Nouvel objet de supervision HP). Dans cet exemple, le rôle regroupera les utilisateurs approuvés pour l'administration du serveur distant. Il sera baptisé *remoteAdmins*. Cliquez sur **OK**.

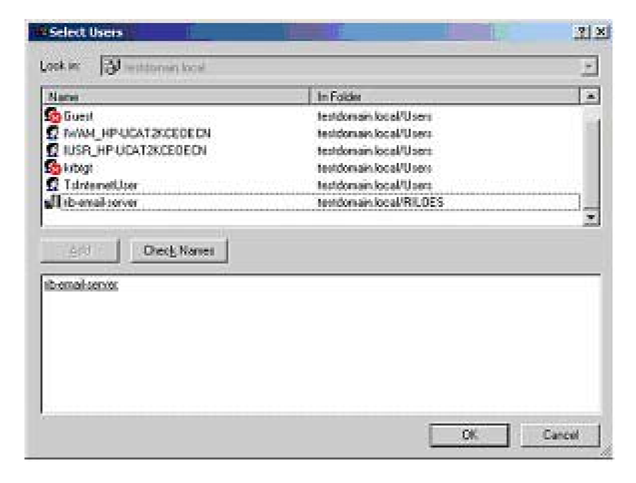
   d. Répétez cette procédure en créant un rôle pour les moniteurs de serveur distant (*remoteMonitors*).

3. Utilisez les composants logiciels intégrables Active Directory Users and Computers (Utilisateurs et ordinateurs) fournis par HP pour attribuer des privilèges de rôle et associer les rôles à des utilisateurs et des périphériques.

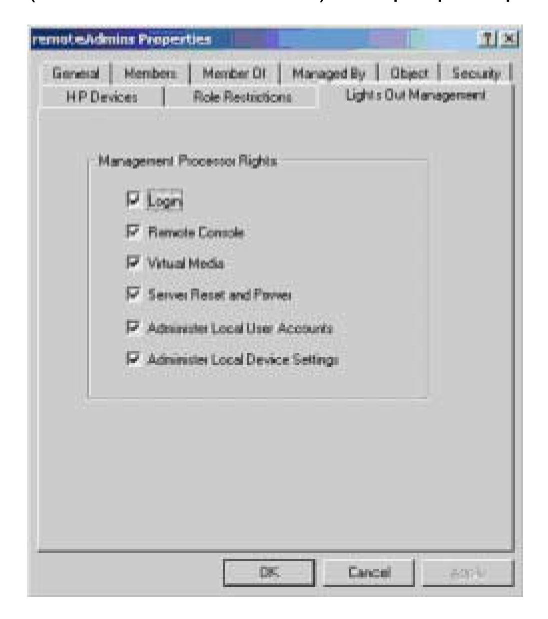
   a. Cliquez avec le bouton droit sur le rôle **remoteAdmins** localisé dans l'unité organisationnelle Roles du domaine *testdomain.local*, puis sélectionnez **Properties** (Propriétés).

   b. Sélectionnez l'onglet **HP Devices** (Périphériques HP), puis cliquez sur **Add** (Ajouter).

   c. Dans la boîte de dialogue Select Users (Sélectionner des utilisateurs), cliquez sur l'objet Lights-Out Management (Supervision Lights-Out) créé à l'étape 2, *rib-email-server*, dans le dossier testdomain.local/RILOES. Cliquez sur **OK** pour fermer la boîte de dialogue, puis sur **Apply** (Appliquer) pour enregistrer la liste.



   d. Ajoutez des utilisateurs au rôle. Cliquez sur l'onglet **Members** (Membres), puis ajoutez des utilisateurs à l'aide du bouton Add (Ajouter) et de la boîte de dialogue Select Users (Sélectionner utilisateurs). Les périphériques et les utilisateurs sont à présent associés.



4. Utilisez l'onglet Lights Out Management (Supervision Lights Out) pour définir les privilèges associés au rôle. Tous les utilisateurs et groupes d'un rôle disposent des privilèges attribués au rôle sur tous les périphériques iLO 2 supervisés par celui-ci. Dans cet exemple, les utilisateurs du

rôle *remoteAdmins* accèdent aux fonctions iLO 2. Cochez les cases en regard de chaque privilège, puis cliquez sur **Apply** (Appliquer). Cliquez sur **OK** pour fermer la feuille des propriétés.

5. En suivant la même procédure que celle décrite à l'étape 4, modifiez les propriétés du rôle *remoteMonitors*, ajoutez le périphérique *rib-email-server* à la liste Managed Devices (Périphériques supervisés) de l'onglet HP Devices (Périphériques HP) et ajoutez des utilisateurs au rôle *remoteMonitors* à l'aide de l'onglet Members (Membres). Puis, dans l'onglet Lights Out Management (Supervision Lights Out), sélectionnez la case en regard de Login (Connexion). Cliquez sur **Apply** (Appliquer), puis sur **OK**. Les membres du rôle *remoteMonitors* pourront désormais s'authentifier et visualiser l'état du serveur.

Les privilèges utilisateur relatifs à un périphérique iLO 2 correspondent à la somme de tous les privilèges attribués par l'ensemble des rôles dont l'utilisateur est membre et dans lesquels le périphérique iLO 2 en question est supervisé. Si l'on se reporte aux exemples précédents, un utilisateur membre à la fois du rôle *remoteAdmins* et de *remoteMonitors* bénéficiera de tous les privilèges, car le rôle *remoteAdmins* lui donne tous ces droits.

Pour configurer un périphérique iLO 2 et l'associer à un objet de supervision Lights-Out utilisé dans cet exemple, il faut recourir à des paramètres similaires à ceux qui sont présentés dans l'écran Directory Settings (Paramètres d'annuaire) ci-dessous.

```
RIB Object DN = cn=rib-email-server,ou=RILOES,dc=testdomain,dc=local
Directory User Context 1 = cn=Users,dc=testdomain,dc=local
```

Par exemple, l'utilisateur *Mel Moore*, possédant le nom unique *MooreM* et localisé dans l'unité organisationnelle users (utilisateurs) du domaine *testdomain.local*, et qui est également membre de l'un des rôles *remoteAdmins* ou *remoteMonitors*, serait autorisé à se connecter à iLO2. Mel entrerait alors `testdomain\moorem` ou `moorem@testdomain.local` ou `Mel Moore` dans le champs Login Name (Nom de connexion) de l'écran de connexion de iLO 2, et utiliserait son mot de passe Active Directory dans le champ Password (Mot de passe) de ce même écran.

Objets de services d'annuaire

Une parfaite virtualisation des périphériques supervisés dans le service d'annuaire constitue l'une des clés de la supervision basée sur les annuaires. Cette virtualisation permet en effet à l'administrateur d'établir des relations entre le périphérique supervisé et les utilisateurs ou groupes déjà présents dans le service d'annuaire. La supervision de la carte iLO 2 par un utilisateur requiert trois objets de base dans le service d'annuaire :

- Supervision Lights-Out
- Rôle
- Utilisateur

Chaque objet représente un périphérique, un utilisateur ou une relation nécessaire pour la supervision basée sur les annuaires.

REMARQUE : une fois les composants logiciels intégrables installés, vous devez redémarrer ConsoleOne et MMC pour visualiser les nouvelles entrées.

Une fois le composant logiciel intégrable installé, vous pouvez créer des objets et des rôles iLO 2 dans l'annuaire. L'outil Users and Computers (Utilisateurs et ordinateurs) permet d'effectuer les tâches suivantes :

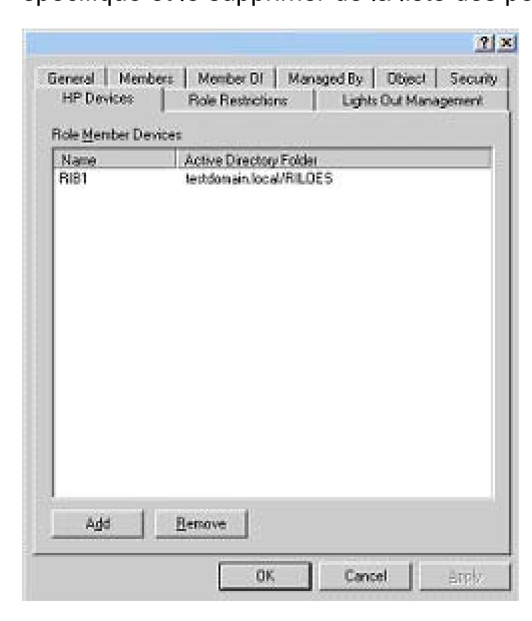
- créer des objets iLO 2 et des objets de rôle ;
- ajouter des utilisateurs aux objets de rôle ;
- définir des privilèges et des restrictions pour les objets de rôle.

Composants logiciels intégrables de Active Directory

Les sections suivantes traitent des options de supervision supplémentaires disponibles dans l'outil Active Directory Users and Computers (Utilisateurs et ordinateurs) après l'installation des composants logiciels intégrables HP.

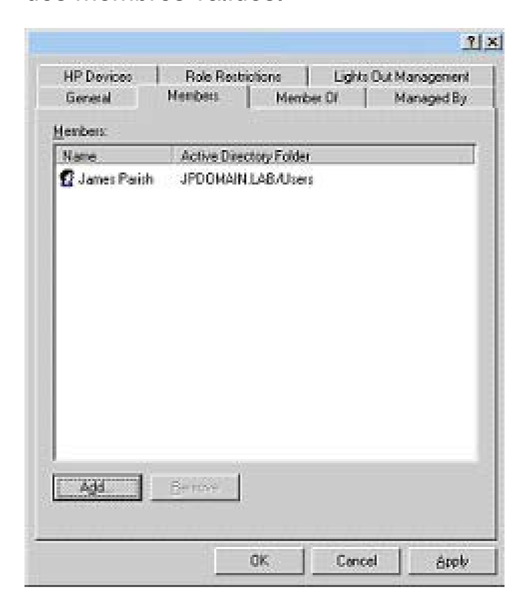
HP Devices (Périphériques HP)

L'onglet HP Devices (Périphériques HP) permet d'ajouter à un rôle des périphériques HP à superviser. Cliquez sur **Add** (Ajouter) pour accéder à un périphérique HP spécifique et l'ajouter à la liste des périphériques membres. Cliquez sur **Remove** (Supprimer) pour accéder à un périphérique HP spécifique et le supprimer de la liste des périphériques membres.



Members (Membres)

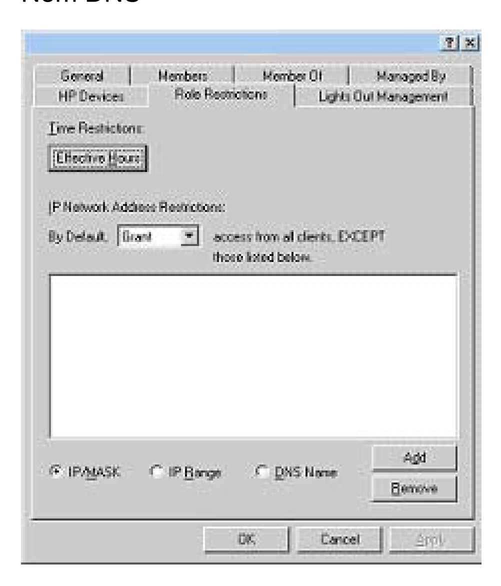
Lorsque des objets utilisateur ont été créés, l'onglet Members (Membres) permet de superviser les utilisateurs appartenant au rôle. Cliquez sur **Add** (Ajouter) pour accéder à l'utilisateur à ajouter. Mettez un utilisateur existant en surbrillance et cliquez sur **Remove** (Supprimer) pour le supprimer de la liste des membres valides.



Restrictions de rôle de la fonction Active Directory

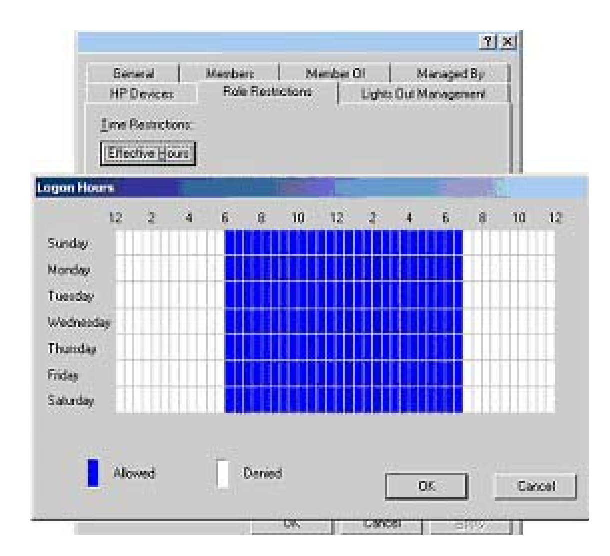
Le sous-onglet Role Restrictions (Restrictions de rôle) permet de définir des restrictions de connexion pour le rôle. Celles-ci incluent :

- Restrictions de temps
- Restrictions liées aux adresses réseau IP
  - IP/Masque
  - Plage d'adresses IP
  - Nom DNS



Restrictions de temps

Vous pouvez superviser les heures de connexion mises à la disposition des membres du rôle en cliquant sur **Effective Hours** (Heures effectives) dans l'onglet Role Restrictions (Restrictions de rôle). La fenêtre contextuelle Logon Hours (Heures de connexion) permet de sélectionner le nombre d'heures disponibles pour la connexion, chaque jour de la semaine, par incréments d'une demi-heure. Vous pouvez modifier un seul carré en cliquant dessus ou modifier un ensemble de carrés en cliquant sur l'un d'eux et en maintenant le bouton de la souris enfoncé, puis en faisant glisser le curseur sur les carrés à modifier et en relâchant le bouton de la souris. Par défaut, l'accès est autorisé en permanence.



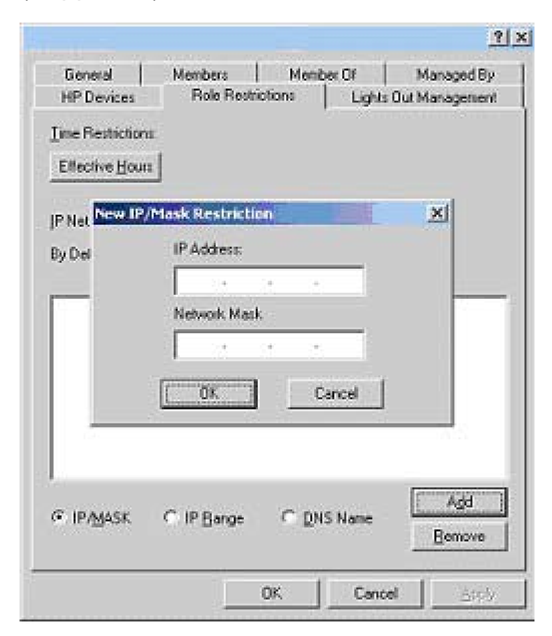
Accès à l'adresse IP ou au nom DNS du client

Il est possible d'accorder ou de refuser l'accès à une adresse IP, une plage d'adresses IP ou des noms DNS.

1. Dans le menu contextuel By Default (Par défaut), sélectionnez **Grant** (Autoriser) ou **Deny** (Refuser) pour autoriser ou refuser l'accès à partir de toutes les adresses, à l'exception des adresses IP, des plages d'adresses IP et des noms DNS spécifiés.
2. Sélectionnez les adresses à ajouter et le type de restriction, puis cliquez sur **Add** (Ajouter).
3. Dans la nouvelle fenêtre contextuelle de restriction, entrez les informations requises et cliquez sur **OK**. La nouvelle fenêtre s'affiche.

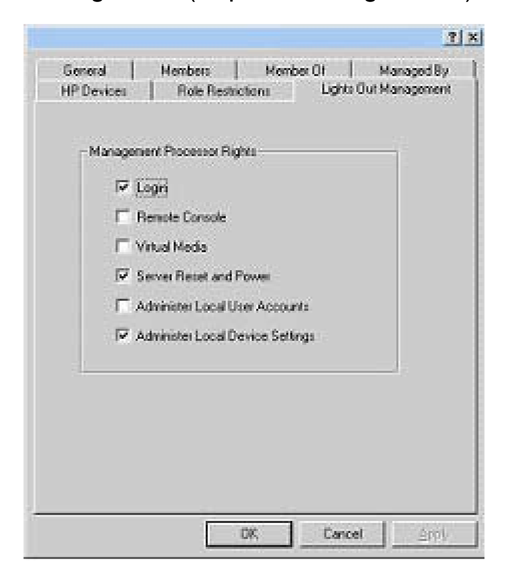
   L'option DNS Name (Nom DNS) permet de limiter l'accès à un nom DNS ou un sous-domaine unique, entré dans le formulaire host.company.com ou *.domain.company.com.
4. Cliquez sur **OK** pour enregistrer les modifications.

Pour supprimer une des entrées, mettez-la en surbrillance dans la liste et cliquez sur **Remove** (Supprimer).



Supervision de Lights-Out dans Active Directory

Après avoir créé un rôle, vous pouvez sélectionner les droits y afférents. Vous pouvez à présent définir les objets Utilisateurs et Groupes comme membres du rôle et attribuer ainsi aux utilisateurs ou à un groupe d'utilisateurs les droits accordés par le rôle. Les privilèges sont gérés dans l'onglet Lights Out Management (Supervision Lights Out).



Les privilèges disponibles sont les suivants :

- **Login** (Connexion) : cette option permet de spécifier si les utilisateurs peuvent accéder ou non aux périphériques associés.
- **Remote Console** (Console distante) : cette option permet à l'utilisateur d'accéder à la console distante.
- **Virtual Media** (Support virtuel) : cette option permet à l'utilisateur d'accéder à la fonction virtual media (support virtuel) de la carte iLO 2.
- **Server Reset and Power** (Réinitialisation et mise sous tension du serveur) : cette option permet à l'utilisateur d'accéder au bouton Virtual Power (Alimentation virtuelle) de la carte iLO 2 afin de réinitialiser le serveur ou de le mettre hors tension à distance.
- **Administer Local User Accounts** (Administrer comptes locaux utilisateur) : cette option permet à l'utilisateur d'administrer ses comptes. Il peut ainsi modifier les paramètres de son propre compte, ceux d'autres comptes, ajouter des utilisateurs ou encore en supprimer.
- **Administer Local Device Settings** (Administrer paramètres du périphérique local) : cette option permet à l'utilisateur de configurer les paramètres du processeur de supervision iLO 2. Ces paramètres incluent les options disponibles dans les écrans Global Settings (Paramètres généraux), Network Settings (Paramètres réseau), SNMP Settings (Paramètres SNMP) et Directory Settings (Paramètres d'annuaire) du navigateur de la carte iLO 2.

Services d'annuaire pour eDirectory

Les sections suivantes décrivent les conditions préalables à l'installation des services d'annuaire pour eDirectory, ainsi que les procédures de préparation et un exemple pratique.

Conditions préalables à l'installation de eDirectory

Les services d'annuaire de la carte iLO 2 utilisent le protocole LDAP sur SSL pour communiquer avec les serveurs d'annuaire. Le logiciel iLO 2 est conçu pour installer une arborescence eDirectory version 8.6.1 et ultérieures. HP déconseille d'installer ce produit si vous possédez des serveurs eDirectory d'une version inférieure à 8.6.1. Avant d'installer les composants logiciels intégrables et les extensions de schéma pour eDirectory, lisez et gardez à disposition les documents d'information techniques suivants, disponibles sur le site Novell Support (http://support.novell.com).

L'installation de la fonction Directory Services (Services d'annuaire) pour la carte iLO 2 requiert l'extension du schéma eDirectory. Cette extension doit être effectuée par un administrateur.

- TID10066591 *Novell eDirectory 8.6 NDS compatibility* (Compatibilité de Novell eDirectory 8.6 NDS)
- TID10057565 *Unknown objects in a mixed environment* (Objets inconnus dans un environnement mixte)
- TID10059954 *How to test whether LDAP is working correctly* (Tester le bon fonctionnement du protocole LDAP)
- TID10023209 *How to configure LDAP for SSL (secure) connections* (Configurer LDAP pour les connexions SSL sécurisées)
- TID10075010 *How to test LDAP authentication* (Tester l'authentification LDAP)

Installation et initialisation des composants logiciels intégrables pour eDirectory

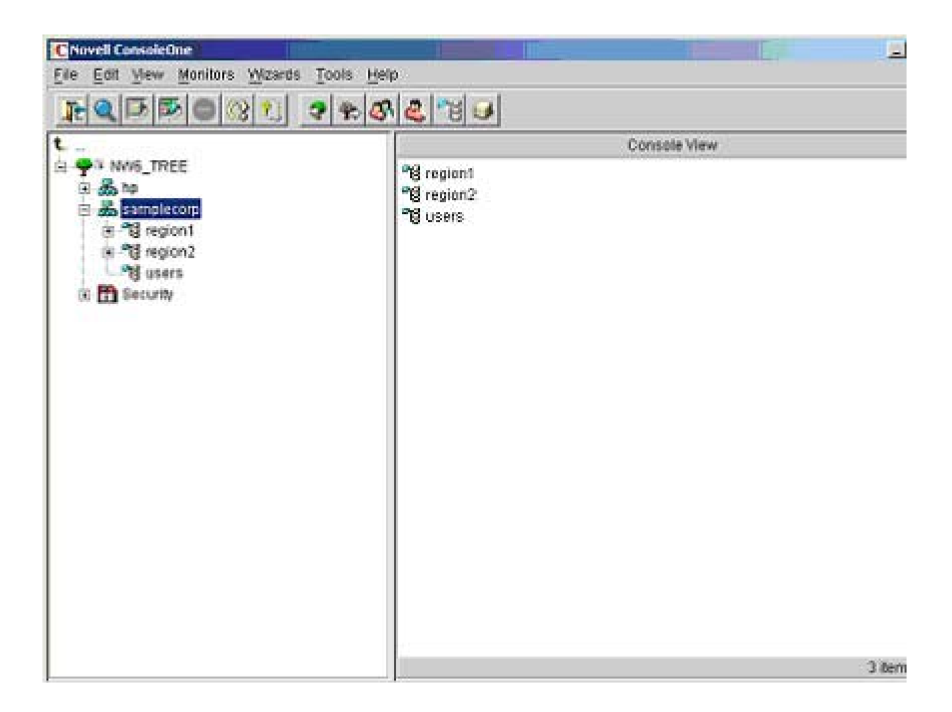
Reportez-vous à la section « Installation et initialisation des composants logiciels intégrables (Installation et initialisation des composants logiciels intégrables pour Active Directory à la page 166) » pour obtenir des informations détaillées sur l'application d'installation des composants logiciels intégrables.

REMARQUE : une fois les composants logiciels intégrables installés, vous devez redémarrer ConsoleOne et MMC pour visualiser les nouvelles entrées.

Exemple : Création et configuration d'objets d'annuaire destinés à être utilisés avec les périphériques LOM dans eDirectory

L'exemple suivant montre comment définir des rôles et des périphériques HP dans une entreprise appelée *samplecorp*, composée de deux régions, *region1* et *region2*.

Supposons que l'annuaire de *samplecorp* soit organisé conformément à l'illustration suivante.



1. Créez des unités organisationnelles dans chaque région. Chacune d'elles est censée contenir les périphériques LOM et les rôles spécifiques à cette région. Dans cet exemple, deux unités organisationnelles sont créées dans « *region1* » et « *region2* » : « *roles* » et « *hp devices* ».

2. Créez les objets LOM dans les unité organisationnelles *hp devices*, pour plusieurs périphériques iLO 2 et à l'aide des logiciels intégrables ConsoleOne fournis par HP.

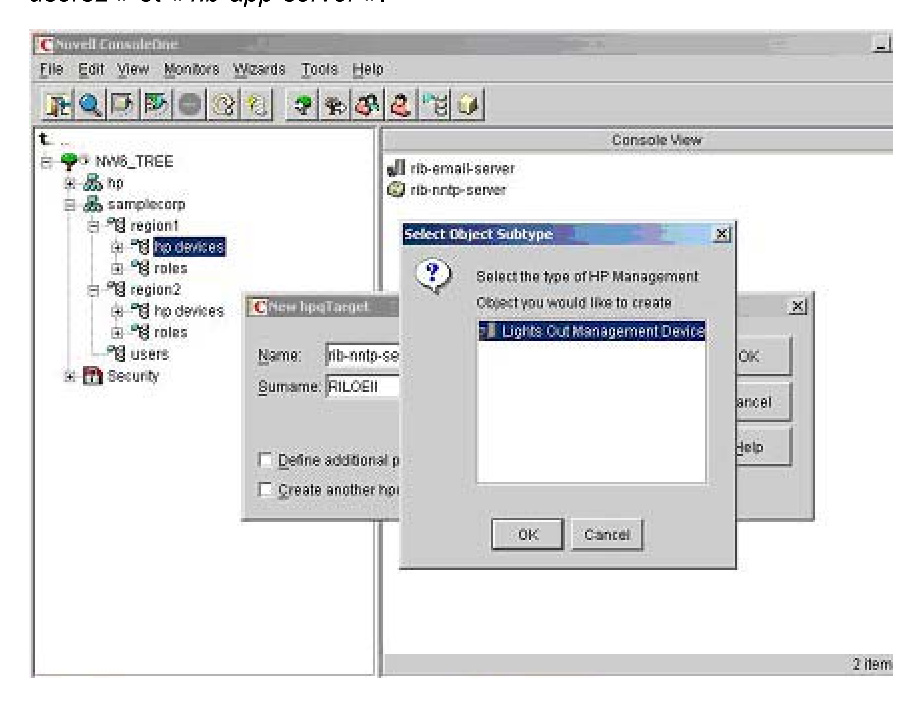
   a. Cliquez avec le bouton droit sur l'unité organisationnelle **hp devices** localisée dans *region1*, puis sélectionnez **New**>**Object** (Nouveau>Objet).

   b. Sélectionnez **hpqTarget** dans la liste de classes, puis cliquez sur **OK**.

   c. Entrez le prénom et le nom de famille appropriés dans la page **New hpqTarget**. Dans cet exemple, le nom d'hôte DNS du périphérique iLO 2, *rib-email-server*, est utilisé comme nom de l'objet LOM, tandis que le nom de famille est *RILOEII*. Cliquez sur **OK**. La page Select Object Subtype (Sélectionner le sous-type de l'objet) s'affiche.

   d. Sélectionnez **Lights Out Management Device** (Périphérique de supervision Lights Out), puis cliquez sur **OK**.

e. Répétez cette procédure pour d'autres périphériques iLO 2, en utilisant les noms DNS « *rib-nntp-server* » et « *rib-file-server-users1* » pour l'unité organisationnelle *hp devices* sous *region1*. Pour l'unité organisationnelle *hp devices* sous *region2*, utilisez « *rib-file-server-users2* » et « *rib-app-server* ».



3. Créez les objets HP Role dans l'unité organisationnelle *roles* à l'aide des logiciels intégrables ConsoleOne fournis par HP.

a. Cliquez avec le bouton droit sur l'unité organisationnelle *roles* localisée dans *region2*, puis sélectionnez *New*>**Object** (Nouveau>Objet).

b. Sélectionnez **hpqRole** dans la liste de classes, puis cliquez sur **OK**.

c. Entrez un nom approprié dans la page **New hpqRole**. Dans cet exemple, le rôle regroupera les utilisateurs approuvés pour l'administration du serveur distant. Il sera baptisé « *remoteAdmins* ». Cliquez sur **OK**. La page Select Object Subtype (Sélectionner le sous-type de l'objet) s'affiche.

d. Dans la mesure où ce rôle doit gérer les privilèges des périphériques de supervision Lights-Out, sélectionnez **Lights Out Management Devices** (Périphériques de supervision Lights Out) dans la liste, puis cliquez sur **OK**.

e. Répétez cette procédure en créant un rôle pour les moniteurs de serveur distant (appelé « *remoteMonitors* ») pour l'unité organisationnelle *roles* sous *region1*, puis les rôles « *remoteAdmins* » et « *remoteMonitors* » pour l'unité organisationnelle *roles* sous *region2*.

4. Affectez des droits au rôle et associez les rôles à des utilisateurs et périphériques à l'aide des logiciels intégrables ConsoleOne fournis par HP.

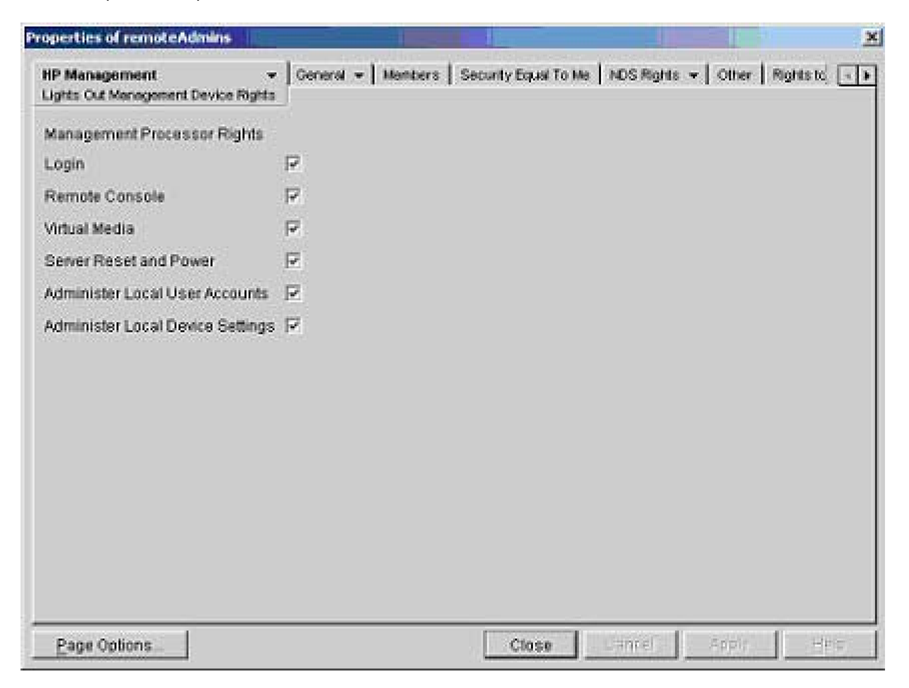
a. Cliquez avec le bouton droit sur le rôle **remoteAdmins**, localisé dans l'unité organisationnelle *roles* sous *region1*, puis sélectionnez **Properties** (Propriétés).

b. Sélectionnez l'onglet **Role Managed Devices** (Périphériques supervisés par le rôle) de l'option HP Management (Supervision HP), puis cliquez sur **Add** (Ajouter).

c. Utilisez la page Select Objects (Sélectionner des objets) pour accéder à l'unité organisationnelle *hp devices* sous *region1*. Sélectionnez les trois objets LOM créés au cours de l'étape 2. Cliquez sur **OK**>**Apply** (OK>Appliquer).

d. Cliquez sur l'onglet **Members** (Membres) et ajoutez des utilisateurs au rôle à l'aide du bouton **Add** (Ajouter) de la page Select Object (Sélectionner un objet). Les périphériques et les utilisateurs sont à présent associés.

e. Définissez les droits associés au rôle à l'aide de l'option Lights Out Management Device Rights (Privilèges des périphériques de supervision Lights Out) de l'onglet HP Management (Supervision HP). Tous les utilisateurs d'un rôle disposent des privilèges attribués au rôle sur tous les périphériques iLO 2 supervisés par celui-ci. Dans cet exemple, les utilisateurs du rôle *remoteAdmins* accèdent aux fonctions iLO 2. Sélectionnez les cases en regard de chaque privilège, puis cliquez sur **Apply** (Appliquer). Pour fermer la feuille des propriétés, cliquez sur **Close** (Fermer).



5. Modifiez les propriétés du rôle *remoteMonitors* en suivant la même procédure que celle décrite à l'étape 4 :

a. Ajoutez les trois périphériques iLO 2 localisés dans l'unité organisationnelle *hp devices* sous *region1* à la liste **Managed Devices** (Périphériques supervisés) de l'option Role Managed Devices (Périphériques supervisés par le rôle), située dans l'onglet HP Management (Supervision HP).

b. Ajoutez des utilisateurs au rôle *remoteMonitors* à l'aide de l'onglet Members (Membres).

c. Cochez la case Login (Connexion), puis cliquez sur **Apply**>**Close** (Appliquer>Fermer). L'option Lights Out Management Device Rights (Privilèges des périphériques de supervision Lights Out) de l'onglet HP Management (Supervision HP) permet aux membres du rôle *remoteMonitors* de s'authentifier et de visualiser l'état du serveur.

Les privilèges utilisateur relatifs à un périphérique LOM correspondent à la somme de tous les privilèges attribués par l'ensemble des rôles dont l'utilisateur est membre et dans lesquels le périphérique LOM en question est supervisé. Si l'on se reporte aux exemples précédents, un utilisateur membre à la fois du rôle *remoteAdmins* et de *remoteMonitors* bénéficiera de tous les privilèges, car le rôle *remoteAdmins* lui donne tous ces droits.

Pour configurer un périphérique LOM et l'associer à un objet de supervision LOM utilisé dans cet exemple, utilisez des paramètres similaires à ceux présentés ci-dessous dans l'écran Directory Settings (Paramètres d'annuaire).

REMARQUE : utilisez des virgules, et non des points, dans les noms distinctifs LDAP pour délimiter chaque composant.

```
RIB Object DN = cn=rib-email-server,ou=hp devices,ou=region1,o=samplecorp
Directory User Context 1 = ou=users,o=samplecorp
```

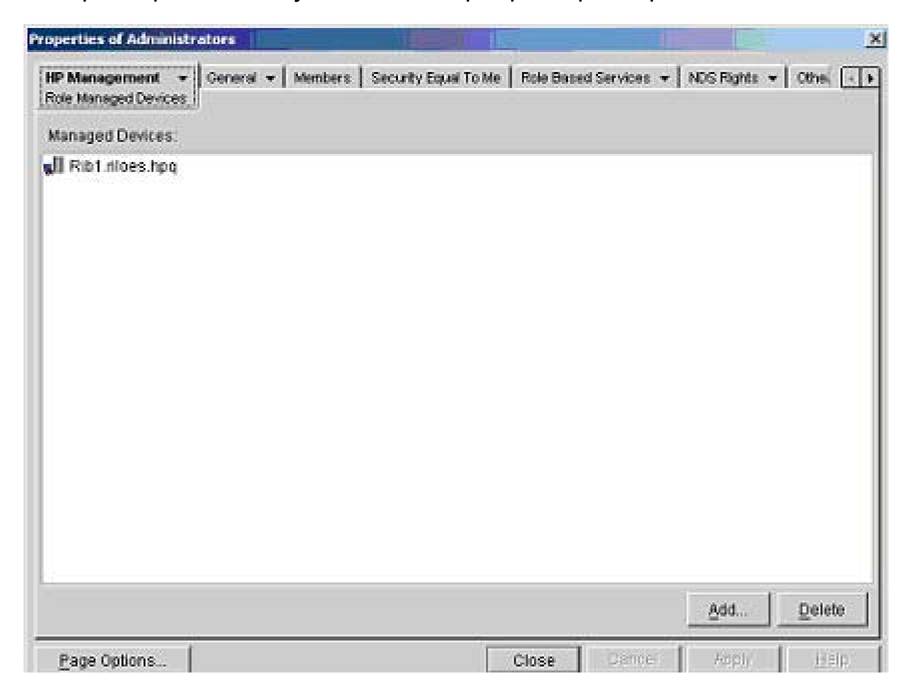
Par exemple, l'utilisateur *CSmith*, localisé dans l'unité organisationnelle *users* (utilisateurs) sous l'organisation *samplecorp*, et qui est également membre du rôle *remoteAdmins* ou de *remoteMonitors*, est autorisé à se connecter à iLO 2. Il doit pour cela entrer `csmith` (insensible à la casse) dans le champ Login Name (Nom de connexion) de l'écran de connexion de iLO 2, puis utiliser le mot de passe eDirectory dans le champ Password (Mot de passe) de ce même écran.

Objets de services d'annuaire pour eDirectory

Les objets de services d'annuaire activent la virtualisation des périphériques supervisés et les relations entre le périphérique supervisé et l'utilisateur ou les groupes déjà présents dans le service d'annuaire.

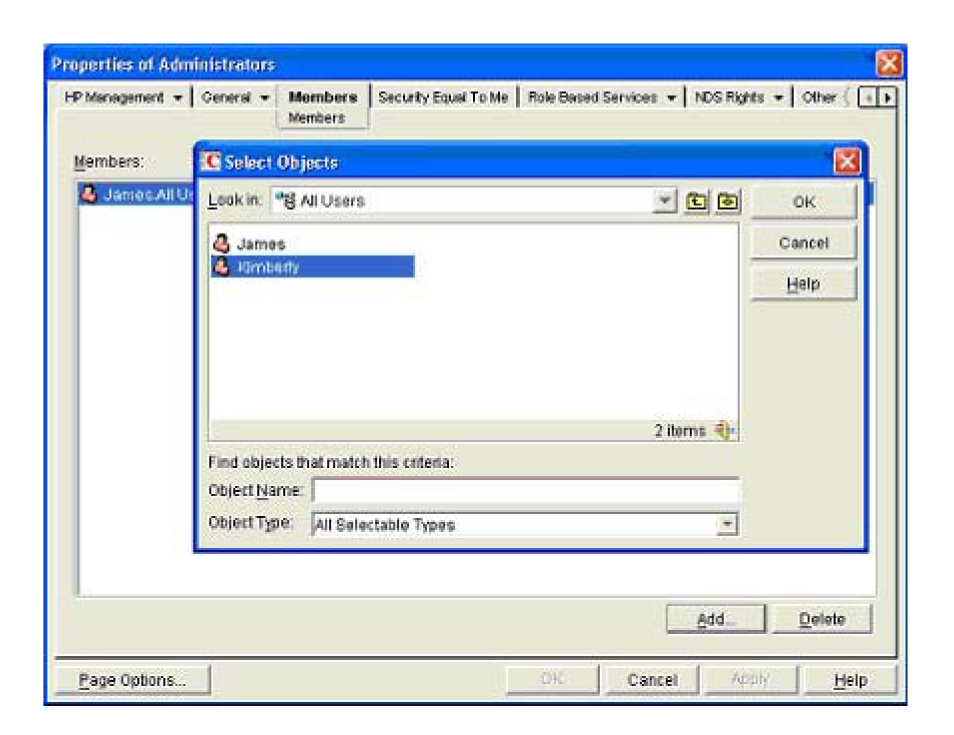
Périphériques supervisés par des rôles

Le sous-onglet Role Managed Devices (Périphériques supervisés par des rôles) permet d'ajouter les périphériques HP à superviser à un rôle. Le bouton **Add** (Ajouter) permet d'accéder à un périphérique HP spécifique, et de l'ajouter comme périphérique supervisé.



Members (Membres)

Une fois que des objets utilisateur ont été créés, l'onglet Members (Membres) permet de superviser les utilisateurs appartenant au rôle. Cliquez sur **Add** (Ajouter) pour accéder à l'utilisateur à ajouter. Mettez un utilisateur existant en surbrillance et cliquez sur **Delete** (Supprimer) pour le supprimer de la liste des membres valides.

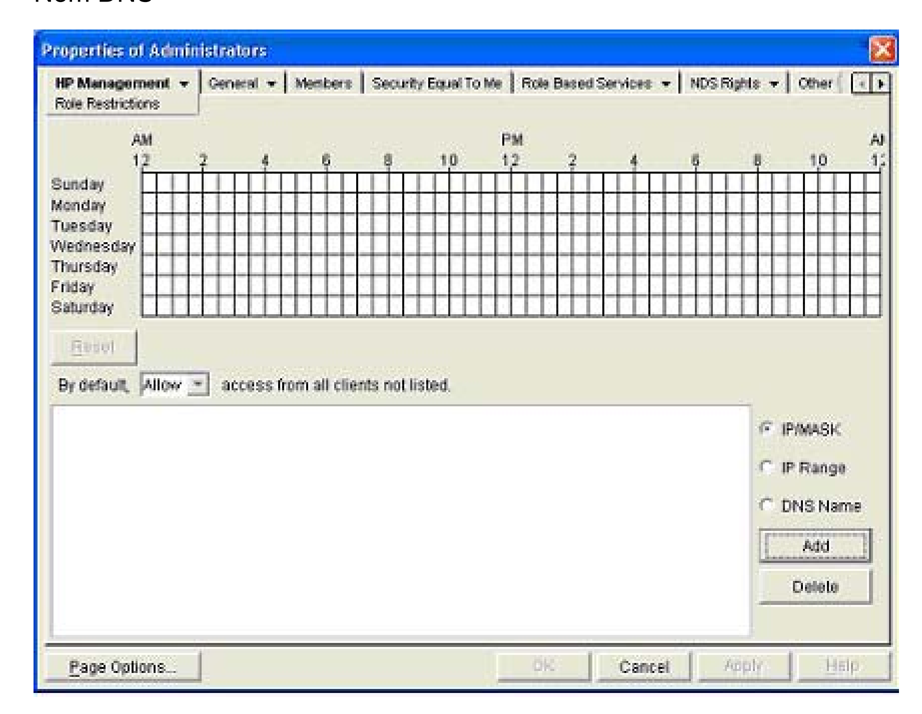


Role Restrictions (Restrictions de rôle) dans eDirectory

Le sous-onglet Role Restrictions (Restrictions de rôle) permet de définir des restrictions de connexion pour le rôle. Celles-ci incluent :

- Restrictions de temps
- Restrictions liées aux adresses réseau IP
  - IP/Masque
  - Plage d'adresses IP

- Nom DNS



Restrictions de temps

Vous pouvez superviser les heures de connexion mises à la disposition des membres du rôle en utilisant la grille horaire affichée dans le sous-onglet Role Restrictions (Restrictions de rôle). Vous pouvez sélectionner les heures de connexion autorisées par incrément d'une demi-heure, et ce, pour chaque jour de la semaine. Vous pouvez modifier l'état d'un carré en cliquant sur celui-ci. Pour un groupe de carrés, cliquez sur le bouton de la souris et maintenez-le enfoncé, faites glisser le curseur sur les carrés à modifier, puis relâchez le bouton de la souris. Par défaut, l'accès est autorisé en permanence.

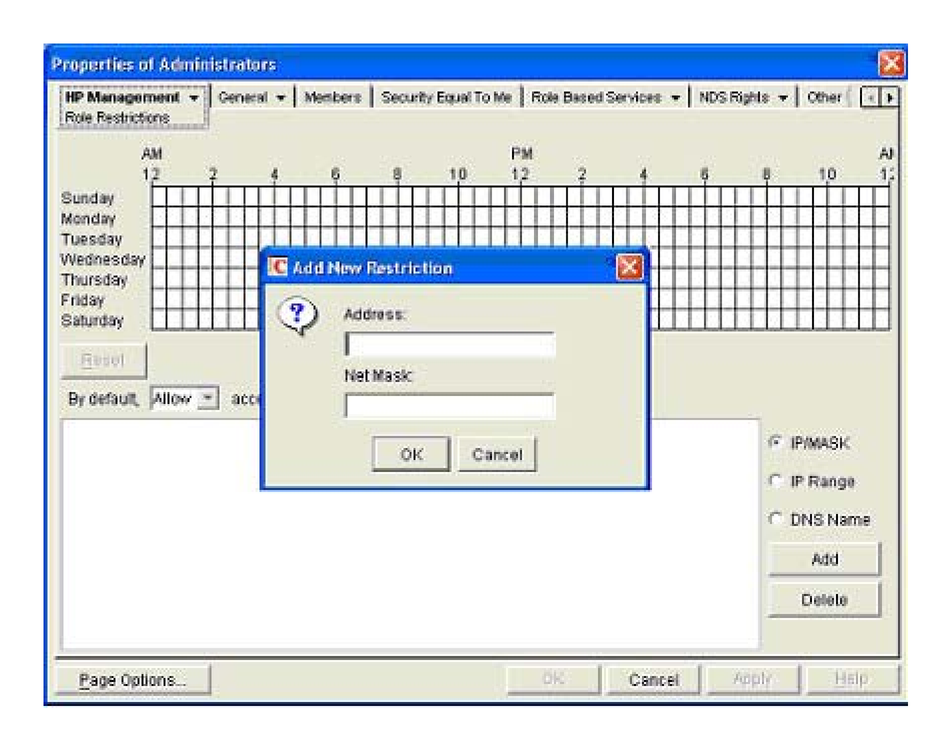
Accès à l'adresse IP ou au nom DNS du client

Il est possible d'accorder ou de refuser l'accès à une adresse IP, une plage d'adresses IP ou des noms DNS.

1. Dans le menu contextuel By Default (Par défaut), sélectionnez **Allow** (Autoriser) ou **Deny** (Refuser) pour autoriser ou refuser l'accès à partir de toutes les adresses, à l'exception des adresses IP, des plages d'adresses IP et des noms DNS spécifiés.
2. Sélectionnez les adresses à ajouter et le type de restriction, puis cliquez sur **Add** (Ajouter).
3. Dans la fenêtre contextuelle Add New Restriction (Ajouter nouvelle restriction), entrez les informations requises et cliquez sur **OK**. La fenêtre contextuelle Add New Restriction (Ajouter nouvelle restriction) de l'option IP/Mask (IP/Masque) s'affiche.

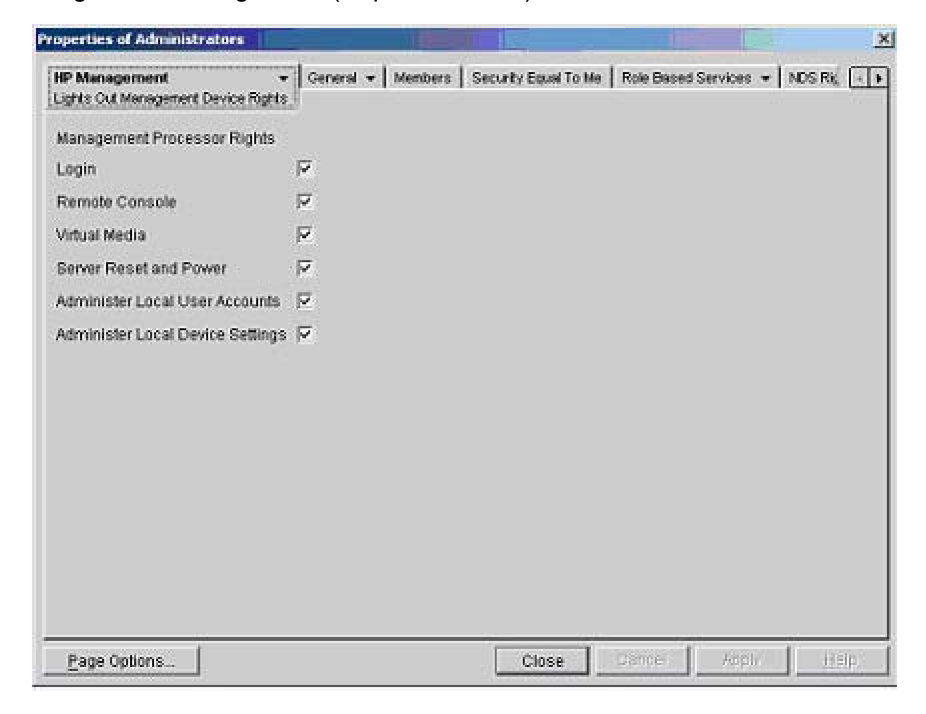
   L'option DNS Name (Nom DNS) permet de limiter l'accès à un nom DNS ou un sous-domaine unique, entré dans le formulaire host.company.com ou *.domain.company.com.
4. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Pour supprimer une entrée, sélectionnez-la dans le champ, puis cliquez sur **Delete** (Supprimer).



eDirectory Lights-Out Management (Supervision eDirectory Lights-Out)

Après avoir créé un rôle, vous pouvez sélectionner les droits y afférents. Vous pouvez à présent définir les objets Utilisateurs et Groupes comme membres du rôle et attribuer ainsi aux utilisateurs ou à un groupe d'utilisateurs les droits accordés par le rôle. La gestion des droits s'effectue dans le sous-onglet Lights Out Management Device Rights (Privilèges des périphériques de supervision Lights Out) de l'onglet HP Management (Supervision HP).



Les privilèges disponibles sont les suivants :

- Login (Connexion) : cette option détermine si les utilisateurs peuvent se connecter aux périphériques associés.

  L'accès à la connexion permet de créer un utilisateur qui est un fournisseur de services et qui reçoit des alertes de iLO 2, mais qui n'a pas accès à iLO 2.
- Remote Console (Console distante) : cette option permet à l'utilisateur d'accéder à la console distante.
- Virtual Media(Support virtuel) : cette option permet à l'utilisateur d'accéder à la fonction de disquette virtuelle et de support virtuel de iLO 2.
- Server Reset and Power (Réinitialisation et mise sous tension du serveur) : cette option permet à l'utilisateur de réinitialiser le serveur ou de le mettre hors tension à distance.
- Administer Local User Accounts (Administrer comptes utilisateur locaux) : cette option permet à l'utilisateur d'administrer des comptes. Il peut ainsi modifier les paramètres de son propre compte, ceux d'autres comptes, ajouter des utilisateurs ou encore en supprimer.
- Administer Local Device Settings (Administrer les paramètres de périphériques locaux) : cette option permet à l'utilisateur de configurer les paramètres de iLO 2. Ces paramètres incluent les options disponibles dans les écrans Global Settings (Paramètres généraux), Network Settings (Paramètres réseau), SNMP Settings (Paramètres SNMP) et Directory Settings (Paramètres d'annuaire) du navigateur iLO 2.

Connexion utilisateur via les services d'annuaire

Le champ Login Name (Nom de connexion) de la page de connexion iLO 2 accepte tous les éléments suivants :

- Utilisateurs d'annuaire
- Noms distinctifs LDAP complets

  Exemple : CN=John Smith,CN=Users,DC=HP,DC=COM ou @HP.com

REMARQUE : la forme simplifiée du nom d'utilisateur n'indique pas à l'annuaire le domaine auquel vous souhaitez accéder. Vous devez fournir le nom du domaine ou utiliser le nom distinctif LDAP de votre compte.

- Forme DOMAINE\nom d'utilisateur (Active Directory uniquement)

  Exemple : HP\jsmith
- Forme nom_utilisateur@domaine (Active Directory uniquement)

  Exemple : jsmith@hp.com

REMARQUE : les utilisateurs d'annuaire spécifiés à l'aide de la forme consultable @ peuvent se trouver dans l'un des trois contextes consultables configurés dans Directory Settings (Paramètres d'annuaire).

- Forme « Nom d'utilisateur »

  Exemple : John Smith

REMARQUE : les utilisateurs d'annuaire spécifiés à l'aide d'une forme du nom d'utilisateur peuvent se trouver dans l'un des trois contextes consultables configurés dans Directory Settings (Paramètres d'annuaire).

- Utilisateurs locaux - Id de connexion

REMARQUE : sur la page de connexion iLO 2, la longueur maximale du nom de connexion est de 39 caractères pour les utilisateurs locaux. Dans le cas des utilisateurs de services d'annuaire, elle est de 256 caractères.

6 Supervision distante activée via l'annuaire

Cette section traite des rubriques suivantes :

Introduction à la supervision distante activée via l'annuaire

Cette section s'adresse aux administrateurs connaissant bien le fonctionnement des services d'annuaire et du produit iLO 2 et qui souhaitent utiliser dans iLO 2 l'option d'intégration d'annuaire dans le cadre du schéma HP. Vous devez comprendre la section « Services d'annuaire (Services d'annuaire à la page 149) » et être capable de reproduire les exemples qui y sont présentés.

La supervision distante activée via l'annuaire permet d'effectuer les tâches suivantes :

- Créer des objets de supervision Lights-Out

  Vous devez créer un objet de périphérique LOM pour représenter chaque périphérique qui utilisera le service d'annuaire pour authentifier et autoriser des utilisateurs. Reportez-vous à la section « Services d'annuaire (Services d'annuaire à la page 149) » pour obtenir des informations supplémentaires sur la création d'objets de périphériques LOM pour Active Directory (Services d'annuaire pour Active Directory à la page 162) et eDirectory (Services d'annuaire pour eDirectory à la page 173). En général, vous pouvez utiliser les composants logiciels intégrables fournis par HP pour créer des objets. Il est utile d'attribuer aux objets de périphérique LOM des noms significatifs, tel que l'adresse réseau du périphérique, le nom DNS, le nom du serveur hôte ou le numéro de série.

- Configurer des périphériques de supervision Lights-Out

  Chaque périphérique LOM utilisant le service d'annuaire pour authentifier et autoriser des utilisateurs doit être configuré avec les paramètres d'annuaire appropriés. Pour obtenir des informations plus détaillées sur les paramètres d'annuaire, reportez-vous à la section « Configuration des paramètres d'annuaire » (Configuration des paramètres d'annuaire à la page 52). En général, vous pouvez configurer chaque périphérique avec l'adresse du serveur d'annuaire appropriée, le nom distinctif de l'objet LOM et tout autre contexte utilisateur. L'adresse du serveur est soit l'adresse IP ou le nom DNS du serveur de l'annuaire local ou pour plus de redondance, un nom DNS multi-hôte.

Création de rôles en fonction de la structure organisationnelle

Souvent, les administrateurs d'une organisation sont placés selon un ordre hiérarchique, dans lequel les administrateurs subordonnés doivent affecter les privilèges indépendamment des administrateurs

responsables. Dans ce cas, il est utile d'avoir un rôle représentant les privilèges affectés par des administrateurs de grade élevé et d'autoriser les administrateurs subordonnés à créer et superviser leurs propres rôles.

Utilisation des groupes existants

De nombreuses organisations voudront répartir leurs utilisateurs et leurs administrateurs en groupes. Dans de nombreux cas, il convient d'utiliser les groupes existants et de les associer avec un ou plusieurs objets de rôle de supervision Lights-Out. Lorsque les périphériques sont associés à des objets de rôle, l'administrateur contrôle l'accès aux périphériques Lights-Out associés au rôle en ajoutant ou supprimant des membres au sein des groupes.

Lors de l'utilisation de Microsoft® Active Directory, il est possible de placer un groupe dans un autre ou des groupes imbriqués. Les objets de rôle sont considérés comme des groupes et peuvent en inclure d'autres directement. Ajoutez directement le groupe imbriqué existant au rôle et affectez les privilèges et les restrictions appropriés. De nouveaux utilisateurs peuvent venir s'ajouter au groupe existant ou au rôle.

Novell eDirectory n'autorise pas l'imbrication des groupes. Dans eDirectory, tout utilisateur pouvant lire un rôle est considéré comme l'un de ses membres. Lors de l'ajout d'un groupe existant, d'une unité organisationnelle ou d'une organisation à un rôle, ajoutez l'objet en tant qu'administrateur en lecture de ce rôle. Tous les membres de cet objet sont considérés comme membres de ce rôle. Il est possible d'ajouter de nouveaux utilisateurs au groupe existant ou au rôle.

Lors de l'utilisation d'affectations de privilèges d'annuaire ou administrateur dans le but d'augmenter le nombre des membres du rôle, les utilisateurs doivent pouvoir lire l'objet LOM correspondant au périphérique LOM. Certains environnements requièrent que les administrateurs d'un rôle soient également administrateurs en lecture de l'objet LOM afin d'authentifier correctement les utilisateurs.

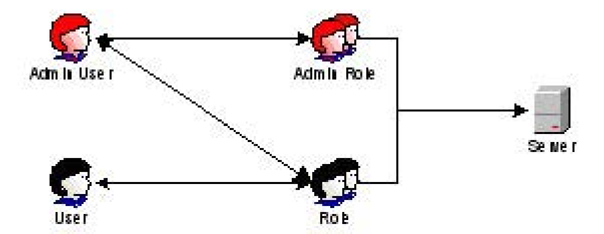
Utilisation des rôles multiples

La plupart des déploiements n'exigent pas qu'un même utilisateur soit dans les différents rôles qui supervisent un périphérique donné. Cependant, ces configurations sont utiles pour la construction de relations de privilèges complexes. Lors de la construction de relations de rôles multiples, les utilisateurs reçoivent tous les privilèges affectés par chaque rôle applicable. Les rôles peuvent uniquement accorder des privilèges mais pas les révoquer. Si un rôle accorde un privilège à un utilisateur, l'utilisateur disposera de ce privilège, même si l'utilisateur appartient, par ailleurs, à un autre rôle qui ne lui accorde pas ce privilège.

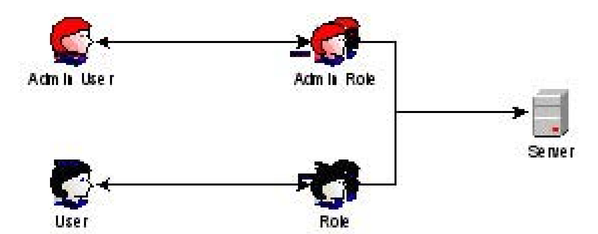
Généralement, un administrateur d'annuaire crée un rôle de base avec un nombre minimum de privilèges affectés, puis il crée des rôles supplémentaires pour ajouter des privilèges supplémentaires. Ces privilèges supplémentaires sont ajoutés dans des circonstances spécifiques ou à un sous-ensemble spécifique d'utilisateurs de rôles de base.

Par exemple, une organisation peut avoir deux types d'utilisateurs, des administrateurs du périphérique LOM ou du serveur hôte et des utilisateurs du périphérique LOM. Dans ce cas, il serait sensé de créer deux rôles, l'un pour les administrateurs et l'autre pour les utilisateurs. Si les deux rôles incluent certains périphériques identiques, ils n'accordent pas les mêmes privilèges. Parfois, il est utile d'affecter des privilèges génériques au rôle de moindre importance et d'y inclure des administrateurs LOM ainsi que le rôle administratif.

Un utilisateur admin accède au privilège de connexion par l'intermédiaire du groupe d'utilisateurs ordinaire. Des privilèges plus avancés sont affectés via Admin role, le rôle administrateur, qui affecte les privilèges supplémentaires : Server Reset (Réinitialisation du serveur) et Remote Console (Console distante).

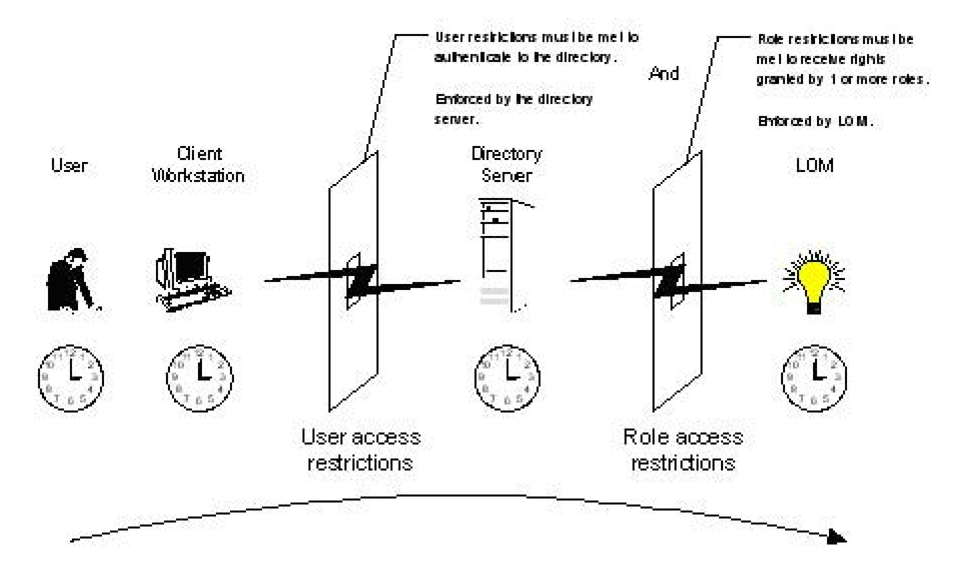


Admin Role, le rôle administrateur, affecte tous les privilèges administrateur : Server Reset (Réinitialisation du serveur), Remote Console (Console distante) et Login (Connexion).



Application des restrictions de connexion à l'annuaire

Il existe deux jeux de restrictions qui limitent potentiellement l'accès d'un utilisateur d'annuaire aux périphériques LOM. Les restrictions d'accès utilisateur limitent l'accès utilisateur à l'authentification de l'annuaire. Les restrictions d'accès de rôle limitent la capacité d'un utilisateur authentifié à recevoir les privilèges LOM, en fonction des privilèges spécifiés dans un ou plusieurs rôles.



Restrictions de rôles

Les restrictions permettent aux administrateurs de limiter le champ d'application d'un rôle. Un rôle n'accorde des privilèges qu'aux utilisateurs satisfaisant aux restrictions du rôle en question. Le recours à des rôles restreints permet de doter les utilisateurs de privilèges dynamiques qui changent en fonction de l'heure de la journée et de l'adresse réseau du client.

REMARQUE : lorsque des répertoires sont activés, l'accès à un iLO 2 donné est basé sur la condition que l'utilisateur a un accès en lecture sur un objet Rôle qui contient l'objet iLO 2 correspondant. Ceci inclut, mais sans s'y limiter, les membres répertoriés dans l'objet Rôle. Si le Rôle est configuré pour permettre aux permissions héritables de se propager à partir d'un parent, les membres du parent qui disposent de privilèges d'accès en lecture auront également accès à iLO 2. Pour afficher la liste des contrôles d'accès, allez dans Users and Computers (Utilisateurs et ordinateurs), ouvrez l'écran de propriétés de l'objet Rôle, puis sélectionnez l'onglet **Security** (Sécurité).

Pour obtenir des instructions détaillées sur la création de restrictions liées à l'heure et au réseau, reportez-vous aux sections « Restrictions de rôle de la fonction Active Directory » Restrictions de rôle de la fonction Active Directory à la page 171) et « Restrictions de rôle dans eDirectory » (Role Restrictions (Restrictions de rôle) dans eDirectory à la page 179).

Restrictions de temps sur les rôles

Les administrateurs peuvent placer des restrictions de temps sur les rôles LOM. Les utilisateurs bénéficient de privilèges spécifiés pour les périphériques LOM listés dans le rôle, seulement s'ils sont membres du rôle et s'ils satisfont aux restrictions de temps définies pour ce rôle.

Les périphériques LOM utilisent le temps de l'hôte local pour appliquer des restrictions de temps. Si l'horloge du périphérique LOM n'est pas réglée, la restriction de temps imposée au rôle échoue, sauf si aucune restriction temporelle n'a été spécifiée pour ce rôle.

Les restrictions de temps basées sur les rôles ne sont satisfaites que si le temps est paramétré sur le périphérique LOM. Le temps est normalement réglé lors de l'amorçage de l'hôte. Il est maintenu par l'exécution des agents du système d'exploitation hôte, qui permet au périphérique LOM de compenser les années bissextiles et minimiser la désynchronisation de l'horloge par rapport à l'hôte. Les événements tels qu'une panne inopinée de courant ou le flashage du microprogramme LOM peuvent empêcher le réglage de l'horloge du périphérique LOM. Le temps de l'hôte doit également être correct afin que le périphérique LOM puisse garder l'heure exacte pendant le flashage du microprogramme.

Restrictions d'adresses de rôles

Les restrictions d'adresses de rôles sont appliquées par le microprogramme LOM, en fonction de l'adresse IP réseau du client. Lorsque les restrictions d'adresses sont satisfaites pour un rôle donné, les privilèges accordés par ce rôle s'appliquent.

Les restrictions d'adresses peuvent être difficiles à gérer si l'accès est tenté via le coupe-feu ou le serveur proxy réseau. Ces deux mécanismes peuvent modifier l'adresse réseau apparente du client, provoquant ainsi l'application des restrictions d'adresses de manière inattendue.

Restrictions utilisateur

Vous avez la possibilité de limiter l'accès à l'annuaire en définissant des restrictions temporelles ou des restrictions liées aux adresses.

Restrictions d'adresses utilisateur

Les administrateurs peuvent placer des restrictions d'adresses réseau sur un compte utilisateur d'annuaire. Ces restrictions sont alors appliquées par le serveur d'annuaire. Reportez-vous à la documentation relative au service d'annuaire pour plus d'informations sur l'application des restrictions d'adresses aux clients LDAP, par exemple pour un utilisateur qui se connecte à un périphérique LOM.

Les restrictions d'adresses réseau placées sur l'utilisateur dans l'annuaire peuvent ne pas s'appliquer comme prévu si l'utilisateur d'annuaire se connecte via un serveur proxy. Lorsqu'un utilisateur se connecte à un périphérique LOM en tant qu'utilisateur d'annuaire, le périphérique LOM tente une authentification sur l'annuaire, en tant qu'utilisateur d'annuaire. Cela signifie que les restrictions

d'adresse placées sur le compte utilisateur s'appliquent lors de l'accès au périphérique LOM. Cependant, du fait que l'utilisateur est relié par un serveur proxy au périphérique LOM, l'adresse réseau de la tentative d'authentification est celle du périphérique LOM et non celle du poste de travail client.

Restrictions de la plage d'adresses IP

Les restrictions de la plage d'adresses IP permettent à l'administrateur de spécifier les adresses réseau dont l'accès est accordé ou refusé par la restriction. La plage d'adresses est généralement spécifiée dans un format de plage inférieur/supérieur. Une plage d'adresses peut être spécifiée pour accorder ou refuser l'accès à une seule adresse. Les adresses appartenant à la plage d'adresses IP inférieure/supérieure obéissent à la restriction d'adresse IP.

Restrictions liées au masque de réseau et à l'adresse IP

Les restrictions liées à l'adresse IP et au masque de sous-réseau permettent à l'administrateur de spécifier une plage d'adresses dont l'accès est accordé ou refusé par la restriction. Ce format possède des capacités similaires à celles d'une plage d'adresses IP mais peut être plus natif pour votre environnement réseau. Une plage d'adresses IP et de masques de sous-réseau est généralement spécifiée à l'aide d'une adresse de sous-réseau et d'une adresse de masque en bit, qui identifie les adresses se trouvant sur le même réseau logique.

En mode binaire, si les bits d'une adresse de système client, augmentée des bits du masque de sous-réseau, correspondent à l'adresse de sous-réseau de restriction, le système client obéit à la restriction.

Restrictions basées sur le protocole DNS

Les restrictions basées sur le protocole DNS utilisent le service d'attribution de nom de réseau pour examiner le nom logique du système client en recherchant les noms de système affectés aux adresses IP du client. Les restrictions DNS requièrent un serveur doté d'un nom fonctionnel. Si le service d'attribution de nom est inaccessible ou en panne, les restrictions DNS ne peuvent être mises en correspondance et elles échouent.

Les restrictions basées sur le protocole DNS peuvent limiter l'accès à un nom de système spécifique ou à des systèmes partageant un suffixe de domaine commun. Par exemple, la restriction DNS www.hp.com correspond à des hôtes auxquels est affecté le nom de domaine www.hp.com. Cependant, la restriction DNS *.hp.com correspond à tous les systèmes HP.

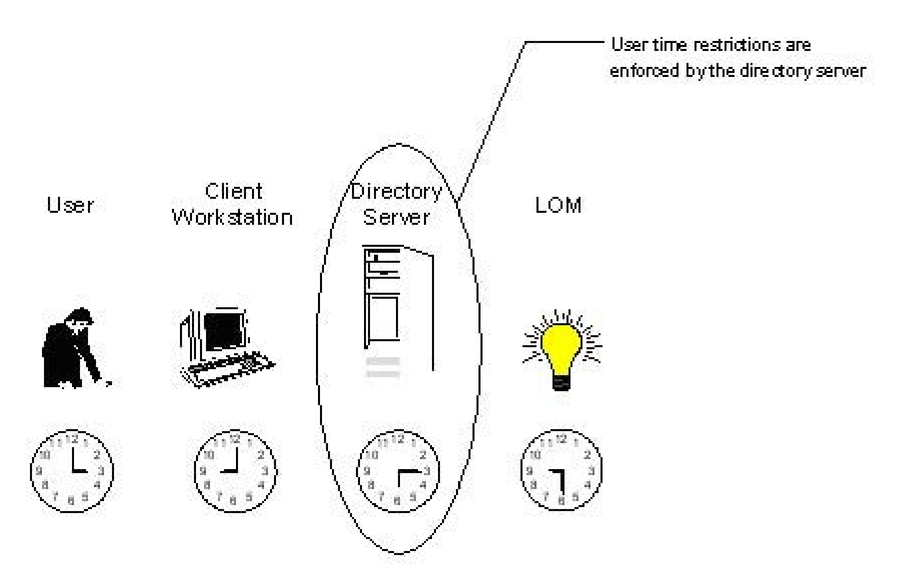
Les restrictions DNS risquent de susciter des ambiguïtés car un système hôte peut avoir plusieurs points d'origine. Les restrictions DNS ne correspondent pas nécessairement en tous points à un seul système.

L'utilisation des restrictions basées sur le protocole DNS peut créer des complications au niveau de la sécurité. Les protocoles de services d'attribution de noms ne sont pas sécurisés. Un individu mal intentionné, ayant accès au réseau, peut placer un service DNS de terminaison sur le réseau, créant de faux critères de restrictions d'adresses. Les stratégies en matière de sécurité organisationnelle devraient être prises en compte lors de l'implémentation de restrictions d'adresses basées sur le protocole DNS.

Application des restrictions de temps à l'utilisateur

Les administrateurs peuvent placer des restrictions de temps sur les comptes des utilisateurs d'annuaire. Les restrictions de temps limitent la capacité de l'utilisateur à se connecter (s'authentifier) à l'annuaire. Généralement, les restrictions de temps sont appliquées à l'aide du temps défini sur le serveur d'annuaire. Cependant, si le serveur d'annuaire est situé dans un fuseau horaire différent ou que l'accès ait lieu à une réplique se trouvant dans fuseau horaire différent, les informations relatives au fuseau horaires émanant de l'objet supervisé pourront être utilisées pour effectuer les ajustements horaires nécessaires.

Le serveur d'annuaire évalue les restrictions de temps utilisateur, mais la détermination peut être compliquée par les changements de fuseau horaire ou le mécanisme d'authentification.



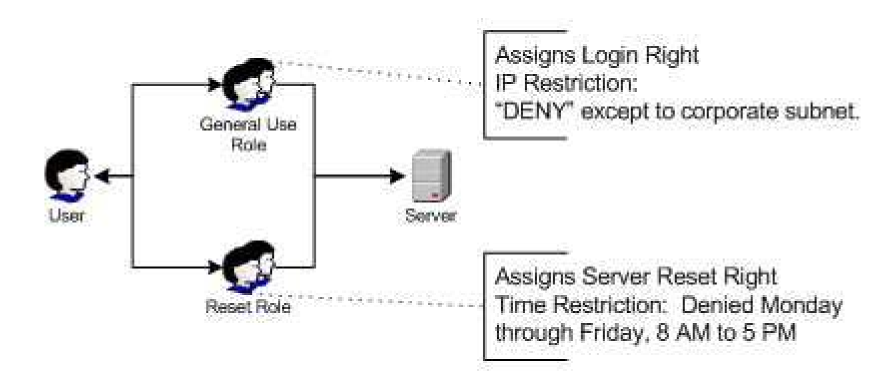
Création de restrictions et de rôles multiples

L'application la plus utile au niveau des rôles multiples consiste à restreindre un ou plusieurs privilèges de sorte que ces derniers ne s'appliquent pas à toutes les situations. D'autres rôles fournissent différents privilèges sous d'autres contraintes. L'utilisation de restrictions et de rôles multiples permet à l'administrateur de créer des relations de privilèges complexes et arbitraires avec un nombre minimum de rôles.

Par exemple, une organisation peut avoir une stratégie de sécurité dans laquelle les administrateurs LOM sont autorisés à utiliser le périphérique LOM à partir du réseau entreprise mais ne peuvent réinitialiser le serveur qu'en dehors des heures ouvrées.

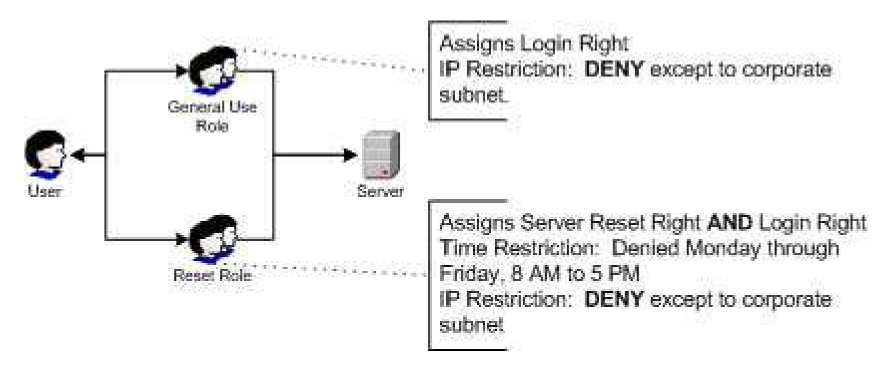
Les administrateurs d'annuaire pourraient être tentés de créer deux rôles pour remédier à cette situation, mais il faut être extrêmement prudent à ce sujet. En effet, créer un rôle fournissant les privilèges de réinitialisation de serveur requis et restreindre son application aux heures non ouvrées permettrait à des administrateurs extérieurs au réseau de l'entreprise de réinitialiser le serveur, ce qui est contraire à la plupart des stratégies de sécurité.

Dans l'exemple donné, la stratégie de sécurité édicte que l'utilisation générale soit restreinte aux clients appartenant au sous-réseau d'entreprise et que la capacité de réinitialisation du serveur soit restreinte, en plus, après les heures d'ouverture normales.



Alternativement, l'administrateur d'annuaire pourrait créer un rôle qui accorderait le privilège de connexion et le restreindrait au réseau d'entreprise, puis en créerait un autre qui accorderait uniquement le privilège de réinitialisation de serveur et en restreindrait l'exercice après les heures d'ouverture normales. Cette configuration est plus facile à superviser mais elle est plus risquée car une administration en continu peut créer un autre rôle qui accorderait le privilège de connexion aux utilisateurs dotés d'adresses extérieures au réseau d'entreprise. Cela pourrait permettre d'accorder, de façon fortuite, aux administrateurs LOM relevant du rôle de réinitialisation du serveur, la capacité de réinitialiser le serveur depuis n'importe où, à condition qu'ils satisfassent aux contraintes de temps spécifiques à ce rôle.

La précédente configuration répond aux exigences de la stratégie de sécurité de l'entreprise. Cependant, le fait d'ajouter un nouveau rôle qui accorderait le privilège de connexion pourrait, par inadvertance, accorder les privilèges de réinitialisation du serveur depuis l'extérieur du sous-réseau d'entreprise après les heures de travail. Une solution plus gérable consisterait à restreindre le rôle Reset (Réinitialisation) ainsi que le rôle General Use (Utilisation générale).



Utilisation des outils d'importation en masse

L'ajout et la configuration d'objets LOM en grand nombre requièrent beaucoup de temps. HP fournit plusieurs utilitaires permettant de vous assister dans ces tâches.

- Utilitaire de migration HP Lights-Out

  HPQLOMIG.EXE, l'utilitaire de migration HP Lights-Out, permet d'importer et de configurer plusieurs périphériques LOM. Il comporte une interface graphique qui fournit une approche étape par étape à l'implémentation ou la mise à niveau des processeurs de supervision en grand nombre. HP recommande d'utiliser cette méthode de l'interface graphique lors de la mise à niveau de plusieurs processeurs de supervision. Pour plus d'informations, reportez-vous à la section « Utilitaire de migration d'annuaire HPQLOMIG » (Utilitaire de migration d'annuaire HPQLOMIG à la page 192).

- Utilitaire de commande de migration Lights-Out HP

  HPQLOMGC.EXE, l'utilitaire de commande de migration Lights-Out HP, offre une approche de la migration basée sur la ligne de commande plutôt que sur l'interface graphique. Cet utilitaire fonctionne conjointement avec les fonctionnalités de lancement des applications et de requête de HP SIM pour configurer simultanément plusieurs périphériques. Les clients qui doivent configurer un nombre limité de périphériques LOM pour utiliser les services d'annuaire peuvent opter pour l'approche de ligne de commande. Pour plus d'informations, reportez-vous à la section « Utilitaire de migration d'annuaire HPQLOMIG » (Utilitaire de migration d'annuaire HPQLOMIG à la page 192).

- Utilitaires HP SIM :
  - supervision de plusieurs périphériques LOM ;
  - identification des périphériques LOM en tant que processeurs de supervision à l'aide de CPQLOCFG pour envoyer un fichier de scripts RIBCL XML vers un groupe de périphériques LOM pour superviser ces derniers. Les processeurs LOM exécutent alors les actions spécifiées dans le fichier RIBCL et envoient une réponse au ficher journal de CPQLOCFG. Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.
- Utilitaires d'importation traditionnels

  Les administrateurs familiarisés avec des outils tels que LDIFDE ou NDS Import/Export Wizard (Assistant d'importation/exportation NDS) peuvent recourir à ces utilitaires pour importer ou créer plusieurs objets de périphériques LOM dans l'annuaire. Toutefois, les administrateurs doivent toujours configurer les périphériques manuellement, comme décrit précédemment, mais peuvent effectuer cette procédure à tout moment. Les interfaces de création de scripts ou de programmes permettent également de créer des objets de périphériques LOM de la même façon que les utilisateurs ou d'autres objets. La section « Schéma des services d'annuaire (Schéma des services d'annuaire à la page 238) » fournit des détails sur les attributs et les formats de données d'attribut pour la création d'objets LOM.

7 Utilitaire de migration d'annuaire HPQLOMIG

Cette section traite des rubriques suivantes :

Présentation de l'utilitaire HPQLOMIG

L'utilitaire HPQLOMIG est destiné aux clients possédant des processeurs de supervision, qui souhaitent simplifier la migration vers la gestion par annuaires. HPQLOMIG automatise certaines des étapes de migration indispensables pour que les processeurs de supervision puissent prendre en charge les services d'annuaire. HPQLOMIG peut effectuer les opérations suivantes :

- détecter les processeurs de supervision sur le réseau ;
- mettre à niveau le microprogramme du processeur de supervision vers une version prenant en charge les services d'annuaire ou les annuaires sans schéma ;
- attribuer un nom aux processeurs de supervision afin de les identifier dans l'annuaire ;
- créer des objets dans l'annuaire correspondant à chaque processeur de supervision et les associer à un rôle ;
- configurer les processeurs de supervision pour leur permettre de communiquer avec l'annuaire.

Compatibilité

L'utilitaire HPQLOMIG fonctionne sous Microsoft® Windows® et nécessite Microsoft® .NET Framework. Pour obtenir plus d'informations et télécharger .NET framework, reportez-vous au site Web de Microsoft® (http://www.microsoft.com/net). L'utilitaire HPQLOMIG prend en charge les systèmes d'exploitation suivants :

- Active Directory
  - Windows® 2000
  - Windows® Server 2003
- Novell eDirectory 8.6.2
  - Windows® 2000
  - Windows® Server™ 2003

Solution HP Lights-Out Directory Package

Tous les logiciels de migration, ainsi que le programmes d'installation du support d'extension de schéma et des composants logiciels intégrables, sont regroupés sous la forme d'un composant HP Smart. Pour compléter la migration des processeurs de supervision, vous devez étendre le schéma et installer les composants logiciels intégrables de supervision avant d'exécuter l'outil de migration. Le composant Smart est situé sur le site Web HP Lights-Out Management (http://www.hp.com/servers/lights-out).

Pour installer les utilitaires de migration, cliquez sur **LDAP Migration Utility** (Utilitaire de migration LDAP) dans le composant Smart. Un programme d'installation Microsoft® MSI est lancé, qui installe l'utilitaire HPQLOMIG, les fichiers DLL requis, le contrat de licence ainsi que d'autres fichiers dans le répertoire C:\Program Files\Hewlett-Packard\HP Lights-Out Migration Tool. Vous pouvez sélectionner un autre répertoire. Le programme d'installation crée un raccourci vers HPQLOMIG sur le menu Démarrer et installe un exemple de fichier XML.

REMARQUE : l'utilitaire d'installation affiche un message d'erreur et se ferme s'il détecte que .NET Framework n'est pas installé.

Utilisation de HPQLOMIG

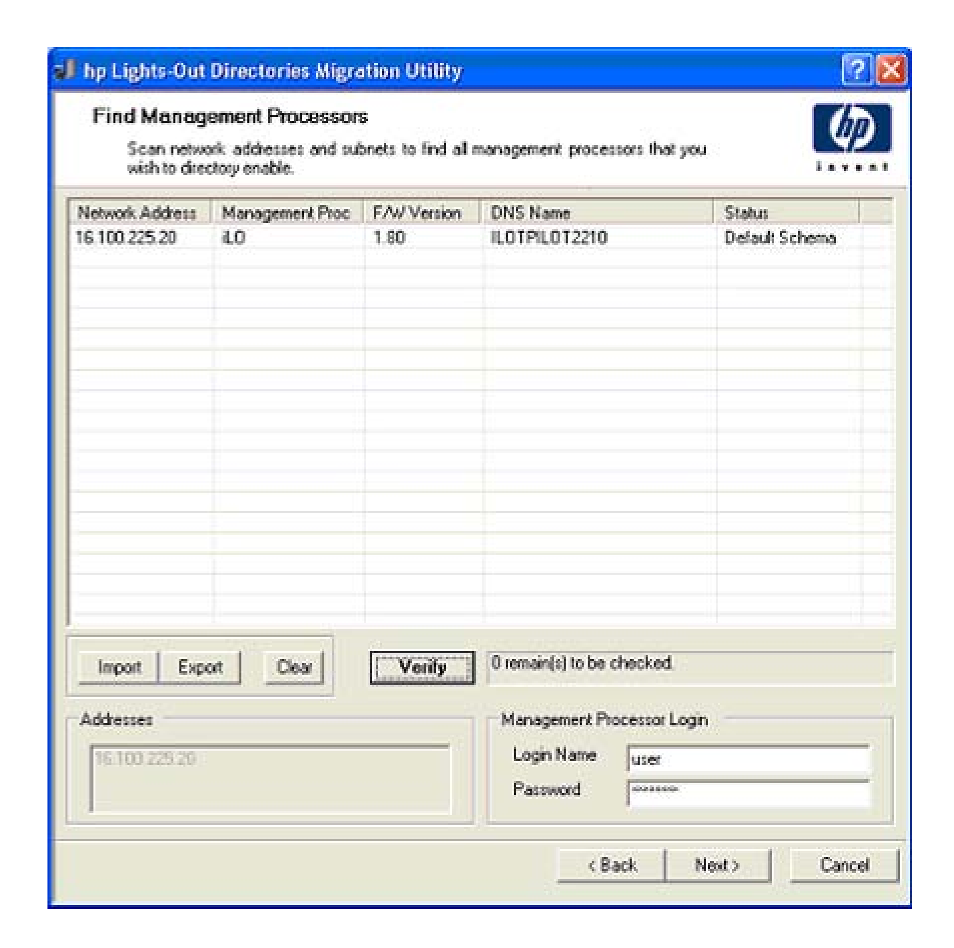
L'utilitaire HPQLOMIG automatise le processus de migration des processeurs de supervision en créant des objets correspondant à chacun des processeurs de supervision dans l'annuaire et en les associant à un rôle. Il est doté d'une GUI et propose à l'utilisateur un assistant pour la mise en œuvre ou la mise à niveau d'une quantité importante de processeurs de supervision.

Localisation de processeurs de supervision

La première étape du processus de migration consiste à localiser tous les processeurs de supervision à activer pour les services d'annuaire. Vous pouvez rechercher les processeurs de supervision à l'aide de noms DNS, d'adresses IP ou de caractères génériques d'adresse IP. Les règles suivantes s'appliquent aux variables entrées dans le champ Addresses (Adresses) :

- Les noms DNS, les adresses IP et les adresses IP en caractères génériques doivent être délimités par un point-virgule.
- Le caractère générique d'adresse IP fait appel au caractère « * » dans les champs des troisième et quatrième octets. Par exemple, l'adresse IP 16.100.*.* est valide alors que l'adresse IP 16.*.*.* ne l'est pas.
- Vous pouvez également préciser des plages de valeurs à l'aide d'un tiret. Par exemple, 192.168.0.2-10 est une plage de valeurs correcte. Le tiret est pris en charge uniquement dans l'octet le plus à droite.
- Une fois que vous avez cliqué sur le bouton **Find** (Rechercher), HPQLOMIG envoie une commande PING et se connecte au port 443 (port SSL par défaut). L'objectif est de déterminer rapidement si l'adresse du réseau cible est un processeur de supervision. Si le périphérique ne répond pas à la commande PING ou ne se connecte pas correctement au port 443, il n'est pas considéré comme un processeur de supervision.

Si vous cliquez sur **Next** (Suivant), **Back** (Précédent) ou que vous quittez l'application en cours de détection, les opérations sur le réseau en cours sont menées à leur terme, mais celles sur les adresses de réseau suivantes sont annulées.



Pour lancer le processus de recherche de vos processeurs de supervision :

1. Pour démarrer la procédure de migration, cliquez sur **Start** (Démarrer), puis sélectionnez **Programs>Hewlett-Packard, Lights-Out Migration Utility** (Programmes>Hewlett-Packard>Utilitaire de migration Lights-Out).
2. Cliquez sur **Next** (Suivant) pour passer outre l'écran d'accueil.
3. Entrez les variables pour exécuter la recherche du processeur de supervision dans le champ Addresses (Adresses).
4. Saisissez votre nom de connexion et votre mot de passe, puis cliquez sur le bouton **Find** (Rechercher). Celui-ci se transforme en bouton Verify (Vérifier) une fois la recherche terminée.

   Vous pouvez également entrer une liste de processeurs de supervision en cliquant sur **Import** (Importer). Le fichier est un simple fichier texte avec un processeur de supervision par ligne. Les champs sont séparés par des points-virgules. Les champs sont les suivants :

   - Network Address (Adresse réseau)
   - Management Processor Type (Type de processeur de supervision)
   - Firmware Version (Version du microprogramme)
   - DNS Name (Nom DNS)
   - User Name (Nom de l'utilisateur)
   - Password (Mot de passe)
   - Directory Configuration (Configuration de l'annuaire)

Par exemple, une ligne peut se présenter comme suit :

```
16.100.225.20;iLO;1.80;ILOTPILOT2210;user;password;Default Schema
```

Si, pour des raisons de sécurité, le nom d'utilisateur et le mot de passe ne peuvent pas figurer dans le fichier, laissez ces champs vides mais conservez les points-virgules.

Mise à niveau du microprogramme des processeurs de supervision

L'écran de mise à niveau du microprogramme permet de mettre à jour les processeurs de supervision à la version du microprogramme qui prend en charge les annuaires. Cet écran permet également de spécifier l'emplacement de l'image du microprogramme pour chaque processeur de supervision en entrant le chemin ou en cliquant sur **Browse** (Parcourir).

REMARQUE : les images binaires du microprogramme des processeurs de supervision doivent être accessibles à partir du système qui exécute l'utilitaire de migration. Ces images binaires peuvent être téléchargées à partir du site Web HP (http://www.hp.com/servers/lights-out).

Processeur de supervision	Version minimale du microprogramme
RILOE	2.50
RILOE II	1.10
iLO	1.40
iLO 2	1.00

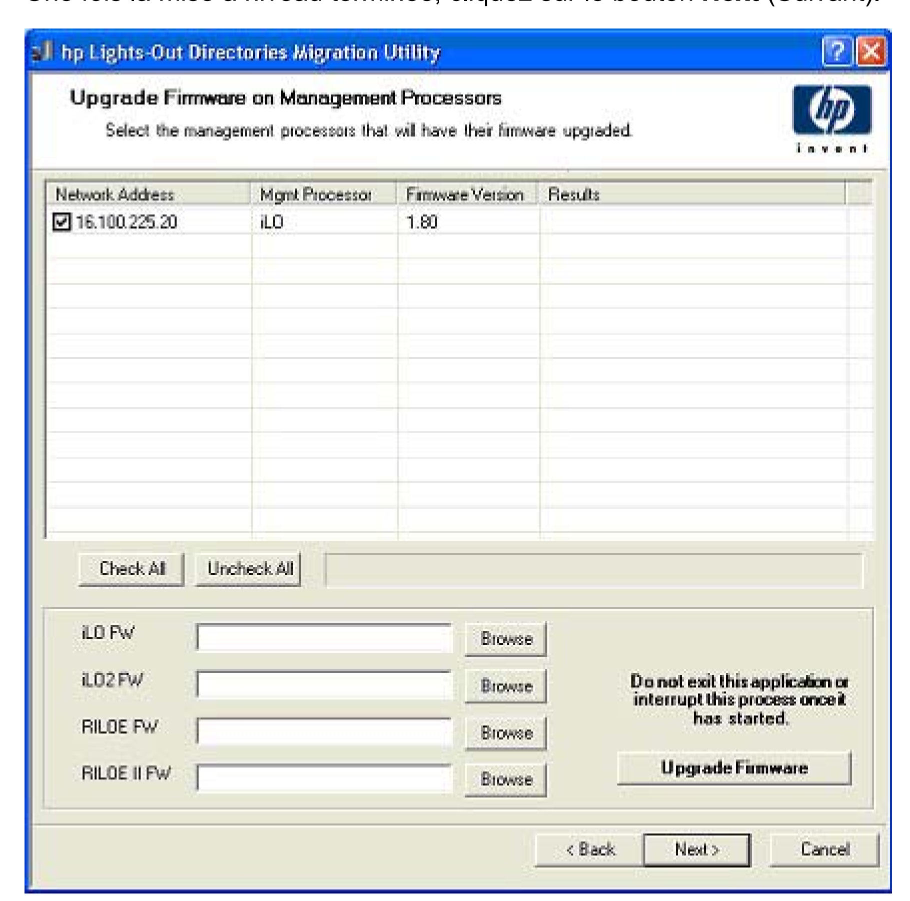
Le processus de mise à niveau peut prendre du temps, selon le nombre de processeurs de supervision sélectionné. La mise à niveau du microprogramme d'un seul processeur de supervision peut prendre jusqu'à cinq minutes. Si la mise à niveau échoue, un message s'affiche dans la colonne Results (Résultats) et l'utilitaire HPQLOMIG continue de mettre à niveau les autres processeurs de supervision identifiés.

REMARQUE : HP vous recommande de tester le processus de mise à niveau et de vérifier les résultats dans un environnement de test avant de lancer l'utilitaire sur un réseau de production. En effet, le transfert incomplet de l'image du microprogramme vers un processeur de supervision pourrait entraîner la reprogrammation locale du processeur de supervision à l'aide d'une disquette.

Pour mettre à niveau le microprogramme de vos processeurs de supervision :

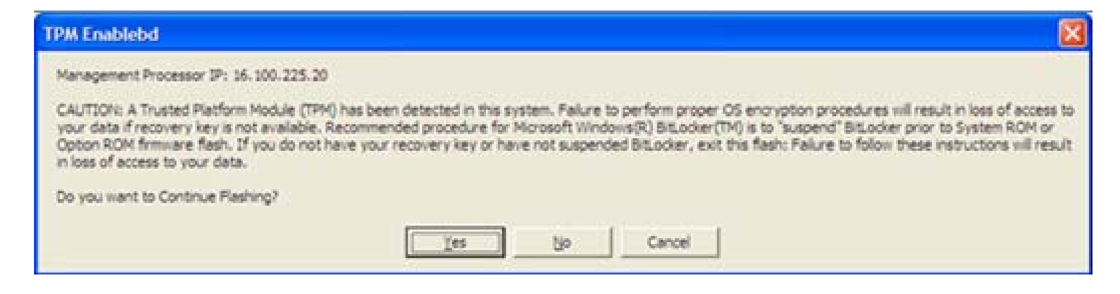
1. Sélectionnez les processeurs de supervision à mettre à niveau.
2. Pour chaque type de processeur de supervision localisé, saisissez le chemin correct vers l'image du microprogramme ou utilisez le bouton Browse (Parcourir) pour l'atteindre.
3. Cliquez sur le bouton **Upgrade Firmware** (Mettre à jour le microprogramme). Les processeurs de supervision sélectionnés sont mis à niveau. Même si cet utilitaire permet de mettre à niveau des centaines de processeurs de supervision, seuls 25 processeurs peuvent être mis à niveau simultanément. L'activité du réseau est considérable pendant la durée de l'opération.

4. Une fois la mise à niveau terminée, cliquez sur le bouton **Next** (Suivant).



Au cours du processus de mise à niveau du microprogramme, tous les boutons sont désactivés pour empêcher la navigation. Vous pouvez tout de même fermer l'application à l'aide du « X » situé dans le coin supérieur droit de l'écran. Si vous fermez l'interface pendant la programmation du microprogramme, l'application continue de fonctionner en arrière-plan et met à niveau le microprogramme sur tous les périphériques sélectionnés.

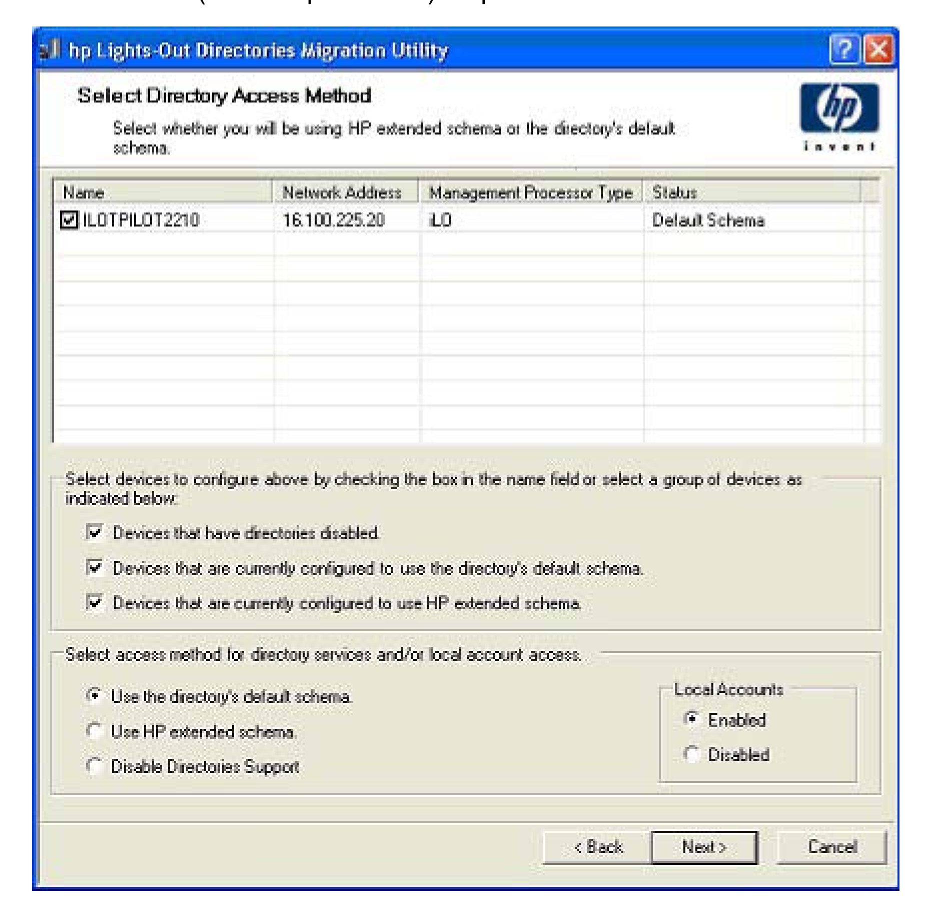
HPLOMIG prend en charge le flashage de microprogramme sur les serveurs dotés d'une puce TPM. Si un module TPM est présent et activé dans le serveur et qu'une mesure de ROM facultative est activée, HPLOMIG affiche un message d'avertissement (illustré ci-dessous.) Si vous sélectionnez Yes (Oui), HPLOMIG continue le processus de flashage. Sinon, le flashage du microprogramme sur le serveur sélectionné est omis. Ce message s'affiche à chaque fois qu'un serveur doté d'un module TPM est détecté au cours du flashage du microprogramme.



Sélection d'une méthode d'accès à l'annuaire

Après la page Firmware Upgrade (Mettre à jour le microprogramme), la page Select Directory Access Method (Sélectionner une méthode d'accès à l'annuaire) s'affiche. Vous pouvez sélectionner les processeurs de supervision à configurer (conformément à l'utilisation ou non du schéma) et la manière dont ils seront configurés. La page Select Directory Access Method (Sélectionner une méthode d'accès à l'annuaire) contribue à empêcher l'écrasement accidentel d'iLO 2 déjà configurés pour un schéma HP ou d'iLO 2 dont les annuaires sont désactivés.

Elle détermine les pages de configuration de la prise en charge qui vont suivre : schéma HP Extended, sans schéma (schéma par défaut) ou pas d'annuaires.



Pour configurer le processeur de supervision pour :

- Directory Services (Services d'annuaire), reportez-vous à la section « Configuration des annuaires avec le schéma HP Extended sélectionné » (Configuration des annuaires avec le schéma HP Extended sélectionné à la page 199).
- La prise en charge d'annuaires sans schéma (schéma par défaut), reportez-vous à la section « Configuration pour l'intégration d'annuaire sans schéma » (Configuration pour l'intégration d'annuaire sans schéma à la page 153).

Attribution de noms aux processeurs de supervision

Cet écran permet d'attribuer un nom aux objets de périphérique Lights-Out Management dans l'annuaire et de créer des objets de périphériques correspondants pour tous les processeurs de supervision à gérer. Vous pouvez créer des noms à l'aide d'un ou de plusieurs des éléments suivants :

- Adresse du réseau
- Nom de DNS
- Un index
- Création manuelle du nom
- Ajout global d'un préfixe
- Ajout global d'un suffixe

Pour attribuer un nom aux processeurs de supervision, cliquez sur le champ **Name** (Nom) et entrez le nom souhaité ou bien :

1. Sélectionnez **Use Network Address** (Utiliser une adresse réseau), **Use DNS Names** (Utiliser des noms DNS), ou **Create Name Using Index** (Créer un nom à partir de l'index). Vous pouvez également nommer chaque objet d'annuaire de processeur de supervision en cliquant deux fois sur le champ du nom, en laissant un petit intervalle de temps entre les clics.
2. Entrez le texte à ajouter (suffixe ou préfixe) à tous les noms (facultatif).
3. Cliquez sur le bouton **Generate Names** (Créer des noms). Les noms s'affichent dans la colonne Name (Nom) dans l'état dans lequel ils sont générés. Pour le moment, les noms ne sont pas écrits dans l'annuaire ou dans les processeurs de supervision. Ils sont stockés jusqu'à la page suivante.
4. Pour changer ces noms (facultatif), cliquez sur le bouton **Clear All Names** (Effacer tous les noms) et attribuez un nouveau nom aux processeurs de supervision.

5. Lorsque les noms sont corrects, cliquez sur le bouton **Next** (Suivant).

Configuration des annuaires avec le schéma HP Extended sélectionné

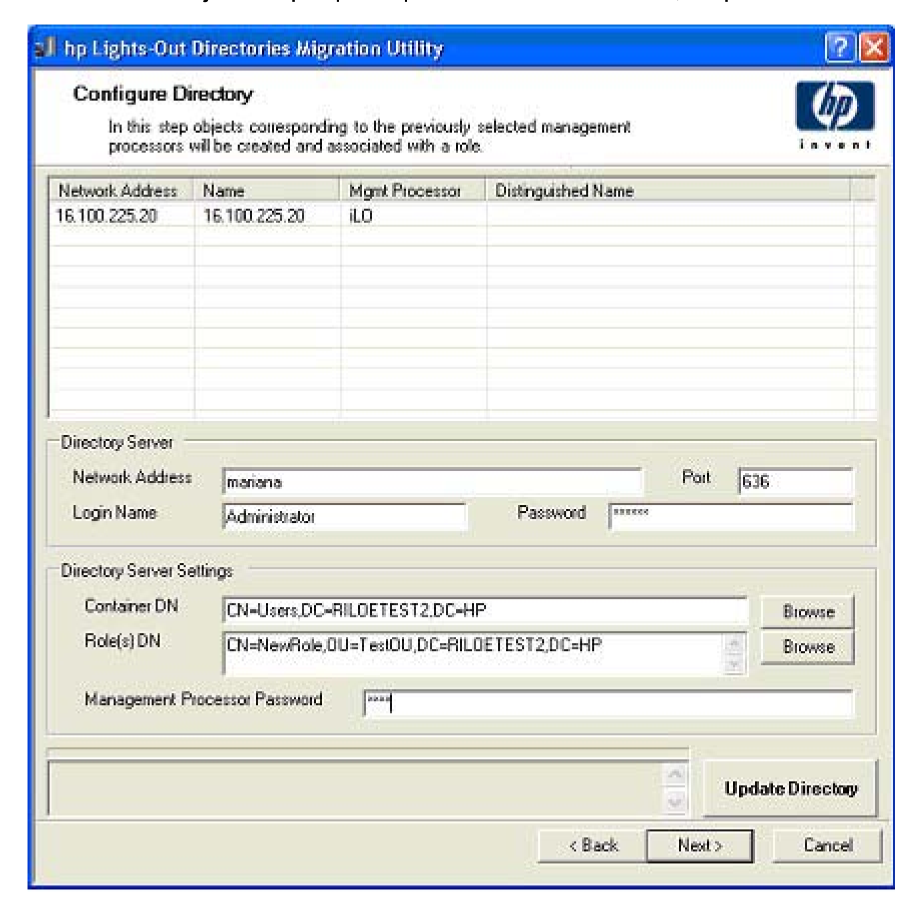
L'écran Configure Directory (Configurer annuaire) permet de créer un objet de périphérique pour chaque processeur de supervision identifié et d'associer ce nouvel objet à un rôle précédemment défini. Par exemple, l'annuaire définit un utilisateur comme étant membre d'un rôle (tel qu'administrateur) disposant d'une série de droits sur un objet de périphérique spécifique (comme une carte RILOE II).

Les champs de l'écran Configure Directory (Configurer annuaire) sont les suivants :

- **Network Address** (Adresse réseau) : adresse réseau du serveur d'annuaire qui peut être une adresse IP ou un nom DNS valide.
- **Port** (Port) : port SSL connecté à l'annuaire. L'entrée par défaut est 636. Les processeurs de supervision peuvent communiquer avec l'annuaire uniquement par le biais du protocole SSL.
- **Login Name** (Nom de connexion) et **Password** (Mot de passe) : ces champs permettent la connexion à l'aide d'un compte doté d'un droit d'accès administrateur de domaine à l'annuaire.
- **Container DN** (Conteneur DN) : une fois que vous disposez des informations relatives à l'adresse réseau, au port et à la connexion, vous pouvez cliquer sur **Browse** (Parcourir) pour accéder au nom distinctif du conteneur et du rôle. Le nom distinctif du conteneur est l'endroit où l'utilitaire de migration va créer tous les objets de processeur de supervision dans l'annuaire.
- **Role DN** (Rôle DN) : le nom distinctif du rôle signale l'emplacement du rôle auquel vont être associés les objets de périphérique. Il doit être créé avant l'exécution de l'utilitaire concerné.

Pour configurer les objets de périphérique à associer à un rôle :

1. Entrez l'adresse réseau, le nom de connexion et le mot de passe pour le serveur d'annuaires spécifié.
2. Entrez le nom distinctif du conteneur dans le champ Container DN (Conteneur DN) ou cliquez sur **Browse** (Parcourir).
3. Associez les objets de périphérique à un membre de rôle en entrant le nom distinctif du rôle dans le champ Role DN (Rôle DN) ou cliquez sur **Browse** (Parcourir).
4. Cliquez sur **Update Directory** (Mettre à jour l'annuaire). L'outil se connecte à l'annuaire, crée les objets de processeur de supervision, puis les ajoute aux rôles sélectionnés.
5. Une fois les objets de périphériques associés à un rôle, cliquez sur le bouton **Next** (Suivant).



Configuration pour l'intégration d'annuaire sans schéma

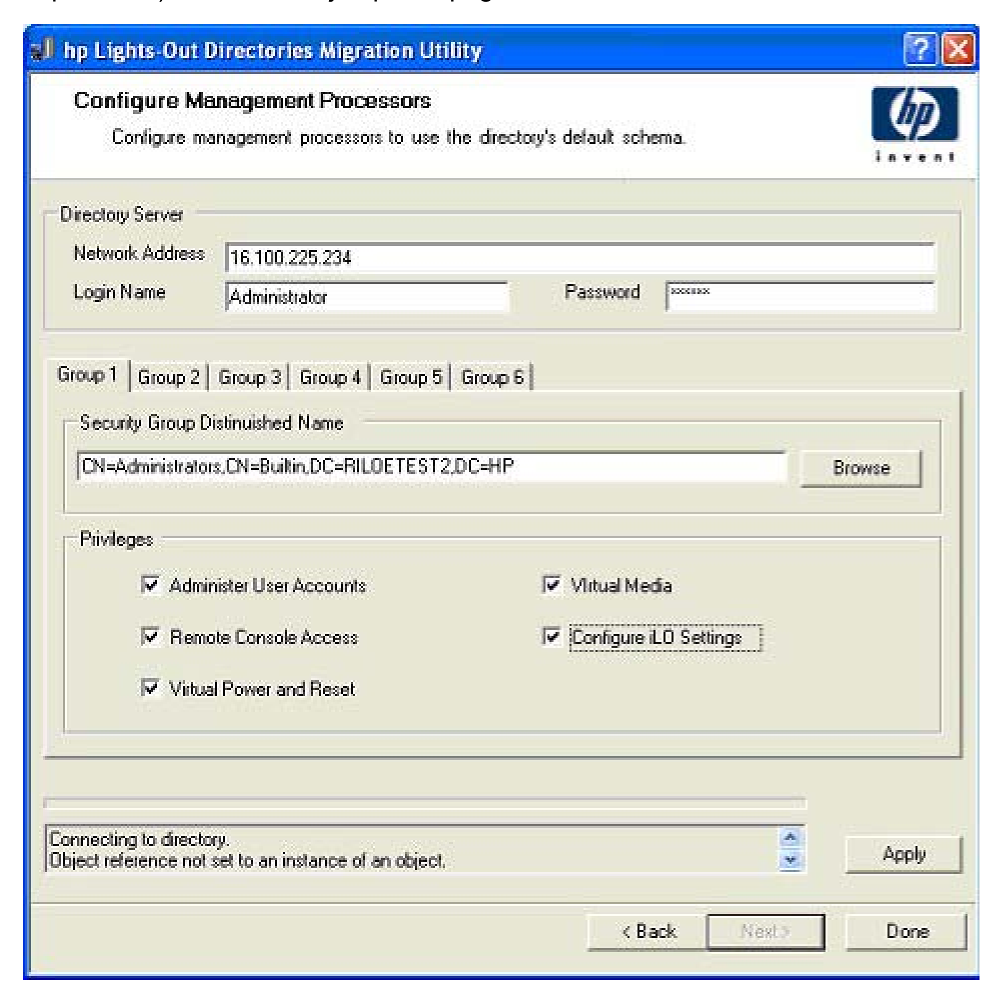
Les champs de l'écran Configure Management Processors (Configurer les processeurs de supervision) sont les suivants :

- **Network Address** (Adresse réseau) : adresse réseau du serveur d'annuaire, qui peut être une adresse IP ou un nom DNS valide.
- **Login Name** (Nom de connexion) et **Password** (Mot de passe) : ces champs permettent la connexion à l'aide d'un compte doté d'un droit d'accès administrateur de domaine à l'annuaire.
- **Security Group Distinguished Name** (Nom distinctif du groupe de sécurité) : nom distinctif du groupe dans l'annuaire qui contient un ensemble d'utilisateurs iLO 2 partageant un ensemble

commun de privilèges. Si le nom d'annuaire, le nom de connexion et le mot de passe sont corrects, vous pouvez cliquer sur le bouton **Browse** (Parcourir) pour accéder au groupe et le sélectionner.

- **Privileges** (Privilèges) : privilèges iLO2 associés au groupe sélectionné. Le privilège de connexion est implicite si l'utilisateur est membre du groupe.

Les réglages du paramètre Configure Management Processors (Configurer les processeurs de supervision) sont stockés jusqu'à la page suivante de l'Assistant.



Configuration des processeurs de supervision pour les annuaires

La dernière étape du processus de migration consiste à configurer les processeurs de supervision pour qu'ils puissent communiquer avec l'annuaire. Cet écran permet de créer des contextes utilisateur.

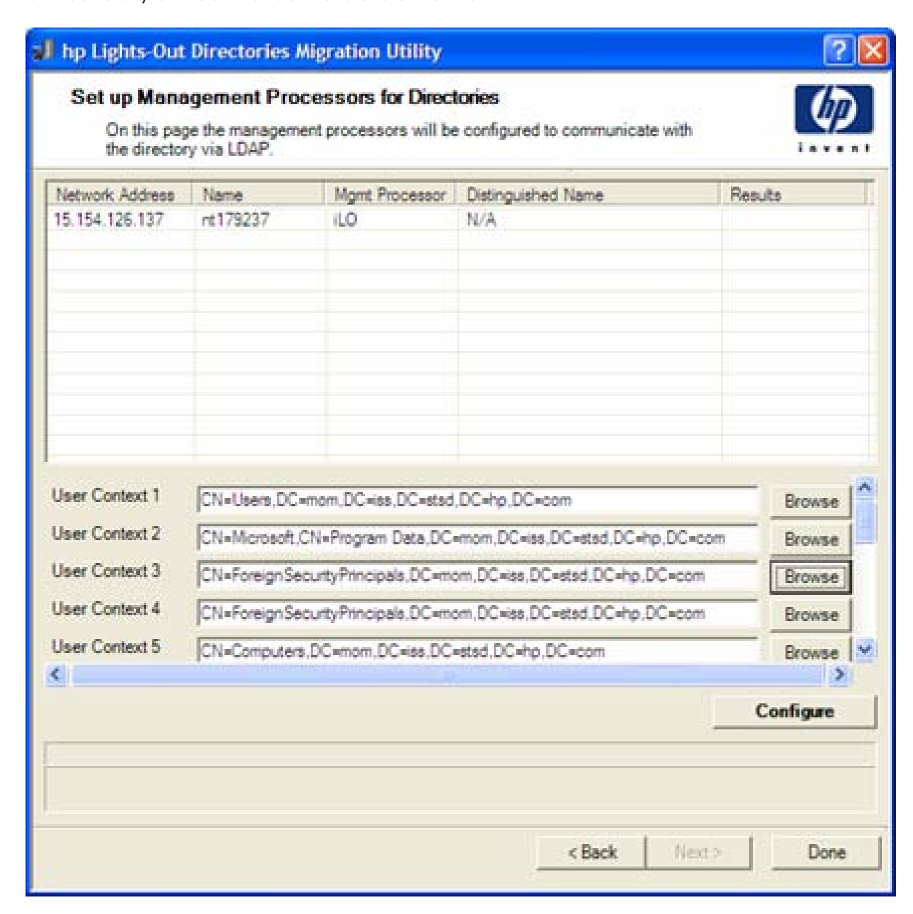
Les contextes utilisateurs permettent d'utiliser un nom abrégé ou un nom d'objet utilisateur pour se connecter, plutôt que le nom distinctif complet. Par exemple, le contexte utilisateur CN=Users,DC=RILOETEST2,DC=HP permet à l'utilisateur « John Smith » de se connecter en tant que John Smith plutôt que CN=John Smith,CN=Users, DC=RILOETEST2,DC=HP. Le format @ est également pris en charge. Par exemple, @RILOETEST2.HP dans un champ de contexte permet à l'utilisateur de se connecter en tant que jsmith (en supposant qu'il s'agit de son nom abrégé).

Pour configurer les processeurs de supervision pour qu'ils communiquent avec l'annuaire :

1. Entrez les contextes utilisateur ou cliquez sur **Browse** (Parcourir).
2. Pour les options Directories Support (Prise en charge des annuaires) et Local Accounts (Comptes locaux), sélectionnez **Enabled** (Activé) ou **Disabled** (Désactivé).

   L'accès distant est désactivé si les deux fonctionnalités Directory Support (Prise en charge des annuaires) et Local Accounts (Comptes locaux) le sont. Pour rétablir l'accès, redémarrez le serveur et utilisez RBSU F8.

3. Cliquez sur **Configure** (Configurer). L'utilitaire de migration se connecte à tous les processeurs de supervision sélectionnés et met à jour leur configuration comme vous l'avez spécifié. HPLOMIG prend en charge la configuration de 15 contextes utilisateur. Pour accéder aux champs de contexte utilisateur, utilisez la barre de défilement.



Lorsque vous cliquez sur Configure (Configurer), HPLOMIG affiche le message suivant :



Le message indique que tous les 15 contextes utilisateur sont applicables uniquement aux machines iLO 2 dotées de la version de microprogramme prise en charge (1.75 ou ultérieure.) Pour tous les autres processeurs de supervision, seuls les trois premiers champs de contexte utilisateur sont applicables.

4. Une fois le processus terminé, cliquez sur le bouton **Done** (Terminé).

8 Intégration de HP SIM (Systems Insight Manager)

Cette section traite des rubriques suivantes :

Intégration d'iLO 2 avec HP SIM

L'intégration d'iLO 2 et de HP SIM dans des environnements d'exploitation clés est totale. L'intégration totale avec Systems Insight Manager offre également une console de supervision unique permettant de lancer un navigateur standard. Lorsque le système d'exploitation est opérationnel, vous pouvez établir une connexion à la carte iLO à l'aide de HP SIM.

L'intégration avec HP SIM offre les fonctionnalités suivantes :

- Prise en charge de SNMP trap delivery (Envoi du trap SNMP) sur une console HP SIM.

  L'envoi de traps SNMP à une console HP SIM peut être configuré pour transférer les traps SNMP vers un pager ou une adresse e-mail.

- Prise en charge de la supervision SNMP.

  HP SIM est autorisé à accéder aux informations des agents Insight Management via iLO 2.

- Prise en charge d'un processeur de supervision.

  HP SIM permet désormais la prise en charge d'un nouveau type de périphérique : le processeur de supervision. Tous les périphériques iLO 2 installés sur des serveurs du réseau sont détectés par HP SIM comme processeurs de supervision. Les processeurs de supervision sont associés aux serveurs sur lesquels ils sont installés.

- Regroupement des processeurs de supervision iLO 2.

  Tous les périphériques iLO 2 peuvent être regroupés logiquement et être affichés sur la même page. Cette capacité permet d'accéder à iLO 2 depuis n'importe quel point de HP SIM.

- Liens hypertexte iLO 2.

  HP SIM offre un hyperlien sur la page Server Device (Périphérique serveur) pour lancer iLO 2 et s'y connecter.

- Agents de supervision HP.

La carte iLO 2, associée aux agents de supervision HP, permet d'accéder à distance aux informations de supervision du système via son interface de navigateur Web.

Présentation fonctionnelle de HP SIM

HP SIM permet les opérations suivantes :

- Identification des processeurs iLO 2.
- Création d'une association entre une carte iLO 2 et son serveur.
- Création de liens entre une carte iLO 2 et son serveur.
- Affichage des informations relatives à iLO 2 et au serveur, ainsi que de leur état.
- Contrôle du niveau de détail affiché pour iLO 2.
- Création de la visualisation de l'infrastructure de rack ProLiant BL p-Class.

Les sections suivantes résument chacune de ces fonctions. Pour obtenir des informations détaillées sur ces avantages et sur les modalités d'utilisation de HP SIM, reportez-vous au manuel *HP Systems Insight Manager Technical Reference Guide* (Manuel de référence technique de HP Systems Insight Manager), fourni avec HP SIM et disponible sur le site Web HP (http://www.hp.com/go/hpsim).

Établissement de SSO avec HP SIM

1. Accédez à une carte iLO 2, puis connectez-vous en utilisant les données d'authentification de l'administrateur.
2. Sélectionnez l'onglet **Administration**.
3. Dans le menu, sélectionnez **Security** (Sécurité).
4. Sélectionnez l'onglet **HP SIM SSO**.
5. Définissez le mode Single Sign-On Trust (Sécuriser authentification unique) sur **Trust by Certificate** (Sécuriser par certificat), puis cliquez sur **Apply** (Appliquer).
6. Cliquez sur **Add HP SIM Server** (Ajouter un serveur HP SIM). La page Single Sign-On Settings (Paramètres d'authentification unique) de HP Systems Insight Manager s'affiche.
7. Dans la section Retrieve and import a certificate from a trusted HP SIM Server (Rechercher et importer un certificat d'un serveur HP SIM agréé), entrez le nom d'hôte ou l'adresse IP du serveur HP SIM, puis cliquez sur **Import Certificate** (Importer certificat). Le serveur est ajouté à la liste des serveurs agréés HP SIM, sous l'onglet HP SIM SSO.
8. Connectez-vous au serveur HP SIM entré au cours de l'étape 7, puis détectez ce serveur <LOM_nom_serveur>. Une fois le processus de détection terminé, SSO est activé pour cette carte iLO 2.

   Pour plus d'informations sur les tâches de localisation, reportez-vous au manuel *HP Systems Insight Manager Technical Reference Guide* (Manuel de référence technique de HP Systems Insight Manager). Pour obtenir plus d'informations sur les options SSO de iLO 2, reportez-vous à la section « Authentification unique HP SIM (HP SIM single sign-on (Authentification unique HP SIM) (SSO) à la page 58). »

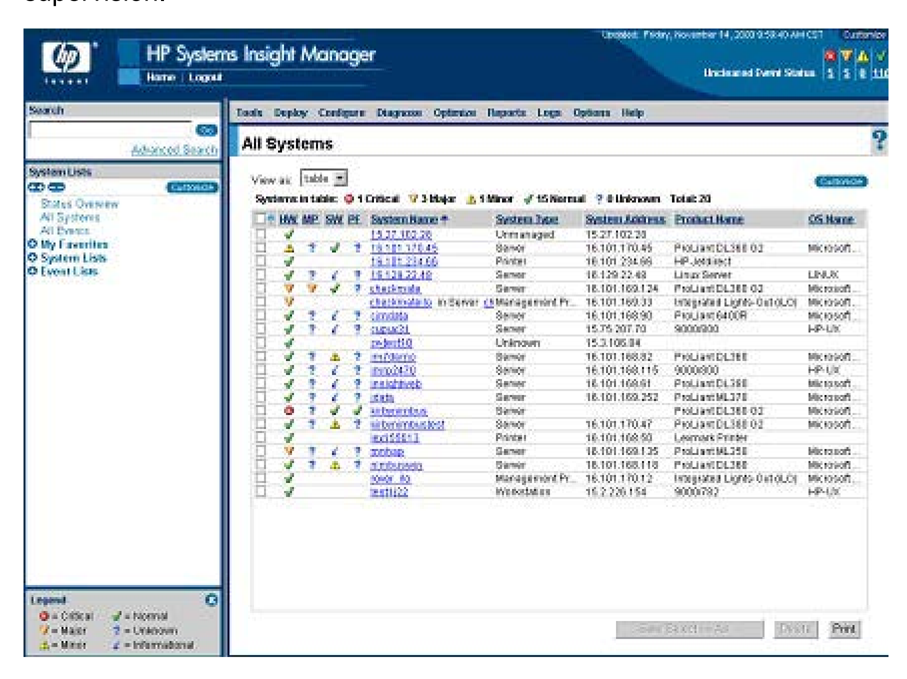
HP SIM : identification et association

HP SIM peut identifier un processeur iLO 2 et créer une association entre iLO 2 et le serveur. L'administrateur du périphérique LOM peut configurer iLO 2 pour répondre aux demandes d'identification de HP SIM.

État de HP SIM

Dans HP SIM, iLO 2 est identifié comme processeur de supervision. HP SIM affiche l'état des processeurs de supervision sur la page Systems List (Liste des systèmes).

Le processeur de supervision iLO 2 apparaît sous la forme d'une icône dans la liste des périphériques, sur la même ligne que son serveur hôte. La couleur de l'icône correspond à l'état du processeur de supervision.



Pour obtenir la liste complète des états de périphérique, reportez-vous au manuel *HP Systems Insight Manager Technical Reference Guide* (Manuel de référence technique de HP Systems Insight Manager), disponible sur le site Web HP (http://www.hp.com/go/hpsim).

Liens de HP SIM

Pour faciliter la supervision, HP SIM crée des liens vers les emplacements suivants :

- la carte iLO 2 et le serveur hôte depuis n'importe quelle liste System (Système) ;
- le serveur depuis la page System (Système) de iLO 2 ;
- la carte iLO 2 depuis la page System (Système) du serveur.

Les pages Systems List (Liste systèmes) affichent la carte iLO 2, le serveur et la relation entre ces deux composants. La page peut, par exemple, afficher le serveur, le nom iLO 2 en regard et la relation *iLO 2 name***IN***server* (nom iLO 2 DANS nom du serveur) dans le champ System Name (Nom de système) correspondant à la carte iLO 2.

Lorsque vous cliquez sur l'icône d'état correspondant à la carte iLO 2, vous accédez à l'interface Web iLO 2. Si vous cliquez sur l'icône d'état du matériel, vous accédez aux agents Insight Management du

périphérique concerné. Cliquez sur iLO 2 ou sur le nom de serveur pour accéder à la page System (Système) du périphérique en question. La page System (Système) comporte les onglets Identity (Identité), Tools & Links (Outils et liens) et Event (Événements). Ces onglets fournissent des informations sur l'identité, l'état, les événements et les liens du périphérique associé.

Liste des systèmes HP SIM

Les processeurs de supervision iLO 2 sont visibles depuis HP SIM. Un utilisateur disposant de tous les droits de configuration peut créer et utiliser des collections de systèmes personnalisées pour les regrouper. Pour obtenir des informations détaillées, reportez-vous au manuel *HP Systems Insight Manager Technical Reference Guide* (Manuel de référence technique de HP Systems Insight Manager), fourni avec HP SIM et disponible sur le site Web HP (http://www.hp.com/go/hpsim).

Réception des alertes SNMP dans HP SIM

Vous pouvez configurer iLO 2 de façon à transférer les alertes à partir des agents de supervision du système d'exploitation de l'hôte et à envoyer à HP SIM les alertes ainsi générées par iLO 2.

HP SIM offre la prise en charge totale de la supervision SNMP, et iLO 2 gère l'envoi du trap SNMP vers HP SIM. Vous pouvez afficher le journal des événements, sélectionner l'événement et afficher des informations complémentaires sur l'alerte.

La configuration de la réception des alertes SNMP dans SIM se décompose en deux étapes. La procédure exige que HP SIM localise, puis configure iLO 2 pour activer les alertes SNMP.

1. Pour permettre à la carte iLO 2 d'envoyer des traps SNMP, cliquez sur l'option **SNMP/Insight Manager Settings** (Paramètres SNMP/Insight Manager), disponible sous l'onglet Administration de la fenêtre de navigation de la carte iLO 2, afin d'activer les alertes SNMP et de fournir une adresse IP de trap SNMP à la carte iLO 2. Cette adresse doit être l'adresse IP de l'ordinateur exécutant HP SIM. Reportez-vous à la section « Activation des alertes SNMP » (Activation des alertes SNMP à la page 70).
2. Pour pouvoir localiser iLO 2 dans HP SIM, vous devez configurer iLO 2 en tant que périphérique supervisé pour HP SIM. L'ajout de la carte iLO 2 à HP SIM permet à l'interface réseau de iLO 2 de fonctionner comme un port de supervision dédié, isolant ainsi le trafic de supervision de l'interface réseau du serveur hôte distant.
   - Démarrez HP SIM.
   - Sélectionnez **Options>Discovery>Automatic Discovery** (Options>Détection>Détection automatique).
   - Sélectionnez la tâche de localisation à exécuter, puis cliquez sur Edit (Modifier).
   - Sélectionnez **IP range pinging** (PING pour plage d'adresses IP). Si l'adresse IP ne se trouve pas dans la plage des adresses susceptibles de répondre à la commande PING, les modèles ou la section des fichiers hôtes, entrez-la manuellement.

- Cliquez sur **OK**.
- Pour ajouter iLO 2 à HP SIM, effectuez l'une des opérations suivantes :
  - Cliquez sur **Save and Run** (Enregistrer et exécuter). Une fois le processus de détection terminé, des requêtes supplémentaires affichent le périphérique en tant que processeur de supervision.

    Il peut s'avérer nécessaire de modifier la « community string » de lecture SNMP (en la remplaçant par « public » par exemple) pour que la carte iLO 2 apparaisse dans la liste des systèmes supervisés. Vous pouvez modifier la chaîne de communauté de lecture SNMP en accédant à la page Systems Protocol Settings (Paramètres de protocole système). Pour accéder à ces paramètres, sélectionnez **Options>Protocol Settings>System Protocol Settings** (Options>Paramètres de protocole>Paramètres de protocole système).
  - Cliquez sur **Options>Protocol Settings>Global Protocol Settings** (Options>Paramètres de protocole>Paramètres généraux de protocole), puis définissez des « community strings » (chaînes de communauté) à utiliser durant la détection sous Default SNMP Settings (Paramètres SNMP par défaut). Une fois la configuration terminée, vous pouvez effectuer les étapes « a » à « e » pour exécuter le processus de détection.

    Pour les événements principaux non effacés, les traps de la carte iLO 2 s'affichent dans All Events (Tous les événements). Pour plus d'informations sur cet événement, cliquez sur **Event Type** (Type de l'événement).

  REMARQUE : les agents de supervision HP Insight pour la carte iLO 2 doivent être installés sur le serveur hôte distant pour que la supervision de iLO 2 soit activée. Pour plus d'informations sur l'installation et la configuration des agents, reportez-vous à la section « Installation des drivers de périphérique iLO 2 ».

Correspondance du port dans HP SIM

HP SIM est configuré pour démarrer une session HTTP et rechercher la carte iLO 2 sur le port 80. Ce port est modifiable. Si vous souhaitez modifier le numéro du port, vous devez également le modifier dans Network Settings (Paramètres réseau) et dans HP SIM.

Pour changer le numéro de port dans HP SIM, ajoutez le port au fichier config\identification \additionalWsDisc.props dans le répertoire où HP SIM est installé. Le port HTTP de la carte iLO 2 doit figurer au début du fichier. Il n'est pas nécessaire d'ajouter ces informations si le numéro de port n'est pas modifié. Il est important que les informations concernant le port figurent sur une seule et même ligne et que le numéro de port soit indiqué en premier. Les autres éléments doivent se présenter sous la forme suivante (la casse doit être respectée) :

L'exemple suivant désigne la configuration de l'entrée si la carte iLO 2 était détectée sur le port 55000 (ces informations doivent tenir sur une seule ligne dans le fichier) :

```
55000=iLO
2, ,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorPa
rser
```

Examen des informations de licence du pack Advanced dans HP SIM

HP SIM affiche l'état de la licence des processeurs de supervision iLO 2. Vous pouvez consulter ces informations pour déterminer le nombre et l'identité des périphériques iLO 2 qui disposent d'une licence du pack iLO Advanced.

Pour afficher les informations de licence, cliquez sur **Deploy>License Manager>Manage Keys** (Déployer>Superviseur de licence>Supervision des clés). Pour s'assurer de la pertinence de ces données, exécutez la tâche d'identification des systèmes pour vos processeurs de supervision. Pour plus d'informations sur le lancement de tâches, reportez-vous à la documentation HP SIM.

9 Résolution des problèmes de la carte iLO 2

Cette section traite des rubriques suivantes :

Voyants POST de iLO 2

Pendant l'amorçage initial du système iLO 2, les voyants POST clignotent pour indiquer la progression du processus. Une fois l'amorçage effectué, le voyant HB (Heartbeat) clignote toutes les secondes. Le voyant 7 clignote aussi à intervalles réguliers pendant le fonctionnement normal.

Les voyants 1 à 6 s'allument après l'initialisation du système pour indiquer une panne du matériel. Réinitialisez iLO 2 si une panne de matériel est détectée. Reportez-vous à la documentation de votre serveur pour connaître l'emplacement des voyants.

Si une panne survient pendant l'exécution de iLO 2, le voyant HB et le voyant 7 restent allumés ou éteints en permanence. Une panne de ce type peut aussi être signalée par le clignotement répété des huit voyants. Si une erreur se produit pendant l'exécution, réinitialisez iLO 2.

Un clignotement séquentiel des voyants 1, 2, 3, 4, 5, 6, 7 et 8, se répétant à l'infini, indique l'échec d'un flashage (mise à niveau du microprogramme) au niveau de la carte iLO 2 et signale que cette dernière est en mode de récupération par flashage. Pour plus d'informations, reportez-vous à la section « Récupération par flashage du réseau de iLO ».

Les voyants ont les affectations suivantes :

HB	7	6	5	4	3	2	1

Voyant	Code POST (activité terminée)	Description	Panne signalée
Aucun	00	Configurer les sélections de puces.	
1 ou 2	02—Fonctionnement normal	Déterminer la plate-forme.	
2 et 1	03	Définir le bit RUNMAP.	
3	04	Initialiser le contrôleur de SDRAM.	
3 et 2	06	Activer le cache I.	
3, 2 et 1	07	Initialiser (uniquement) le cache D.	
4	08	Copier le chargeur secondaire dans la RAM.	Impossibilité de copier le chargeur secondaire.
4 et 1	09	Vérifier le chargeur secondaire.	Défaut d'exécution du chargeur secondaire.
4 et 2	0a	Lancer le chargeur secondaire.	Échec du test de la mémoire SDRAM.
4, 2 et 1	0b	Copier la ROM dans la RAM.	Impossibilité de copier le bloc d'amorçage.
4 et 3	0c	Vérifier l'image de la ROM dans la RAM.	Échec de l'exécution du bloc d'amorçage.
4, 3 et 1	0d	Main du bloc d'amorçage démarré.	Le bloc d'amorçage n'a pas trouvé d'image valide.
Aucun		Démarrer l'initialisation de C Runtime.	
4, 3 et 2	0e	Main() a reçu le contrôle.	Échec de l'autotest de Main.
Variable	Variable	Chaque sous-système peut effectuer un auto-test.	
4, 3, 2 et 1	0f	Démarrer ThreadX	Échec du démarrage de RTOS.
Aucun	00	Main_init() terminé	Échec du démarrage du sous-système.
HB et 7		Clignote pendant que le processeur iLO 2 exécute le code du microprogramme. Ne change pas la valeur des six voyants inférieurs.	

Le microprogramme du microprocesseur iLO 2 comporte un code qui effectue des contrôles de cohérence. En cas d'échec de l'un de ces contrôles, le microprocesseur exécute le FEH. Le FEH présente les informations au moyen des voyants POST de iLO 2. Les codes FEH se distinguent par le clignotement alternatif du numéro 99 et du reste du code d'erreur.

Code FEH	Contrôle de cohérence	Explication
9902	TXAPICHK	Une fonction RTOS a été appelée avec une valeur inadéquate ou à partir d'un appelant inapproprié.
9903	TXCONTEXT	Le contenu enregistré d'un ou plusieurs threads a été altéré.
9905	TRAP	Le test d'une pile a échoué, l'adresse de retour n'est pas valide ou une instruction de trap non valide a été détectée.
9966	NMIWR	Une écriture inattendue a été effectuée dans la mémoire basse.
99C1	CHKNULL	Le vecteur de réinitialisation a été modifié.

Entrées du journal d'événements

Affichage du journal d'événements	Explication
Server power failed (Panne d'alimentation du serveur)	S'affiche lorsque l'alimentation du serveur tombe en panne.
Browser login (Ouverture de session via le navigateur) : *Adresse IP*	Affiche l'adresse IP du navigateur qui a ouvert la session.
Server power restored (Alimentation du serveur rétablie)	S'affiche lorsque l'alimentation du serveur est rétablie.
Browser logout (Fermeture de session via le navigateur) : *Adresse IP*	Affiche l'adresse IP du navigateur qui a fermé la session.
Server reset (Serveur réinitialisé)	S'affiche lorsque le serveur est réinitialisé.
Failed Browser login - IP Address (Échec d'ouverture de session via le navigateur - adresse IP) : *Adresse IP*	S'affiche lorsque l'ouverture de session par un navigateur échoue.
iLO 2 Self-Test Error (Erreur de l'auto-test iLO 2) : #	S'affiche lorsque iLO 2 a échoué lors d'un test interne. La cause probable est la panne d'un composant critique. HP vous déconseille de continuer à utiliser iLO 2 sur ce serveur.
iLO 2 reset (iLO 2 réinitialisé)	S'affiche lorsque iLO 2 est réinitialisé.
On-board clock set; was (Horloge intégrée mise à l'heure ; l'heure était) #:#:#:#:#:#	S'affiche lorsque l'horloge intégrée est mise à l'heure.
Server logged critical error(s) (Erreur(s) critique(s) enregistrées par le serveur)	S'affiche lorsque le serveur enregistre des erreurs critiques.
Event log cleared by (Journal d'événements effacé par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur efface le journal d'événements.
iLO 2 reset to factory defaults (iLO 2 réinitialisé avec les valeurs d'usine)	S'affiche lorsque les paramètres par défaut de iLO 2 sont restaurés.
iLO 2 ROM upgrade to # (Mise à niveau de la ROM iLO 2 avec la version No)	S'affiche lorsque la ROM a été mise à niveau.
iLO 2 reset for ROM upgrade (iLO 2 réinitialisé après mise à niveau de la ROM)	S'affiche lorsque iLO 2 est réinitialisé pour une mise à niveau de la ROM.
iLO reset by user diagnostics (iLO 2 réinitialisé par les diagnostics utilisateur)	S'affiche lorsque iLO 2 est réinitialisé par un diagnostic utilisateur.

Affichage du journal d'événements	Explication
Power restored to iLO 2 (Alimentation de iLO 2 rétablie)	S'affiche lorsque l'alimentation de iLO 2 est rétablie.
iLO 2 reset by watchdog (iLO 2 réinitialisé par l'horloge de surveillance)	S'affiche lorsqu'une erreur s'est produite dans iLO 2 et que iLO 2 s'est réinitialisé. Si l'erreur persiste, contactez l'assistance technique.
iLO 2 reset by host (iLO 2 réinitialisé par l'hôte)	S'affiche lorsque le serveur réinitialise iLO 2.
Recoverable iLO 2 error, code # (Erreur iLO 2 récupérable, code No)	S'affiche lorsqu'une erreur non critique s'est produite dans iLO 2 et que iLO 2 s'est réinitialisé. Si l'erreur persiste, contactez l'assistance technique.
SNMP trap delivery failure (Échec d'envoi du trap SNMP) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Test SNMP trap alert failed for (Échec de l'alerte du trap SNMP de test pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Power outage SNMP trap alert failed for (Échec de l'alerte du trap SNMP de coupure d'alimentation pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Server reset SNMP trap alert failed for (Échec de l'alerte du trap SNMP de réinitialisation de serveur pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Illegal login SNMP trap alert failed for (Échec de l'alerte du trap SNMP d'ouverture de session illégale pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Diagnostic error SNMP trap alert failed for (Échec de l'alerte du trap SNMP d'erreur de diagnostic pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Host generated SNMP trap alert failed for (Échec de l'alerte du trap SNMP généré par l'hôte pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Network resource shortage SNMP trap alert failed for (Échec de l'alerte du trap SNMP de manque de ressources réseau pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
iLO 2 network link up (Lien réseau iLO 2 activé)	S'affiche lorsque le réseau est connecté à iLO 2.
iLO 2 network link down (Lien réseau iLO 2 désactivé)	S'affiche lorsque le réseau n'est pas connecté à iLO 2.
iLO 2 Firmware upgrade started by (Mise à niveau du microprogramme iLO 2 initiée par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur lance la mise à niveau d'un microprogramme.
Host server reset by (Serveur hôte réinitialisé par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur réinitialise le serveur hôte.
Host server powered OFF by (Serveur hôte mis hors tension par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur met un serveur hôte hors tension.
Host server powered ON by (Serveur hôte mis sous tension par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur met un serveur hôte en tension.
Virtual Floppy in use by (Disquette virtuelle utilisée par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur commence à utiliser une disquette virtuelle.
Remote Console login (Ouverture de session sur la console distante) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur ouvre une session sur une console distante.
Remote Console Closed (Console distante fermée)	S'affiche lorsqu'une session d'une console distante est fermée.
Failed Console login - IP Address (Échec d'ouverture de session sur la console distante - adresse IP) : *Adresse IP*	Affiche le nom et l'adresse IP utilisés pour une tentative d'ouverture de session sur une console distante qui a échoué.
Added User (Utilisateur ajouté) : *User (Utilisateur)*	S'affiche en cas d'ajout d'un utilisateur local.

Affichage du journal d'événements	Explication
User Deleted by (Utilisateur supprimé par) : *User (Utilisateur)*	S'affiche en cas de suppression d'un utilisateur local.
Modified User (Utilisateur modifié) : *User (Utilisateur)*	S'affiche en cas de modification d'un utilisateur local.
Browser login (Ouverture de session via le navigateur) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur valide ouvre une session iLO 2 à l'aide d'un navigateur Internet.
Browser logout (Fermeture de session via le navigateur) : User (Utilisateur)	S'affiche lorsqu'un utilisateur ferme une session iLO 2 à l'aide d'un navigateur Internet.
Failed Browser login - IP Address (Échec d'ouverture de session via le navigateur - adresse IP) : *Adresse IP*	S'affiche lorsque l'ouverture de session par un navigateur échoue.
Remote Console login (Ouverture de session sur la console distante) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur autorisé ouvre une session à l'aide du port de la console distante.
Remote Console Closed (Console distante fermée)	S'affiche lorsqu'un utilisateur autorisé de la console distante a fermé une session ou lorsque le port de la console distante est fermé à la suite d'une tentative d'ouverture de session manquée.
Failed Console login - IP Address (Échec d'ouverture de session par la console distante - adresse IP) : *Adresse IP*	S'affiche lorsqu'un utilisateur non autorisé a échoué dans trois essais d'ouverture de session en utilisant le port de la console distante.
Added User (Utilisateur ajouté) : *User (Utilisateur)*	S'affiche lorsqu'une nouvelle entrée est portée à la liste des utilisateurs non autorisés.
User Deleted by (Utilisateur supprimé par) : *User (Utilisateur)*	S'affiche lorsqu'une entrée est retirée de la liste des utilisateurs non autorisés. La section Utilisateur affiche l'utilisateur qui a demandé la suppression.
Event Log Cleared (Journal d'événement effacé) : *User (Utilisateur)*	S'affiche lorsque l'utilisateur efface le journal d'événements.
Power Cycle (Reset) (Cycle d'alimentation - Réinitialisation) : *User (Utilisateur)*	S'affiche lorsque l'alimentation a été réinitialisée.
Virtual Power Event (Événement d'alimentation virtuelle) : *User (Utilisateur)*	S'affiche en cas d'utilisation du bouton virtuel d'alimentation.
Security Override Switch Setting is On (Le commutateur de neutralisation de la sécurité est activé)	S'affiche lorsque le système est amorcé tandis que le commutateur de neutralisation de la sécurité est activé.
Security Override Switch Setting Changed to Off (Passage du commutateur de neutralisation de la sécurité de l'état activé à l'état désactivé)	S'affiche lorsque le système est amorcé avec passage du commutateur de neutralisation de l'état activé à l'état désactivé.
On-board clock set; was previously [NOT SET] (Horloge intégrée mise à l'heure ; l'heure était auparavant [NON DÉFINIE])	S'affiche lorsque l'horloge intégrée est mise à l'heure. Affiche l'heure précédente ou l'indication "NOT SET" (Non définie) si l'heure n'avait pas été définie auparavant.
Logs full SNMP trap alert failed for (Échec de l'alerte du trap SNMP de saturation des journaux) : *Adresse IP*	S'affiche lorsque les journaux sont saturés et que l'alerte du trap SNMP a échoué pour une adresse IP spécifiée.
Security disabled SNMP trap alert failed for (Échec de l'alerte du trap SNMP de désactivation de la sécurité pour) : *Adresse IP*	S'affiche lorsque la sécurité a été désactivée et que l'alerte du trap SNMP a échoué pour une adresse IP spécifiée.
Security enabled SNMP trap alert failed for (Échec de l'alerte du trap SNMP d'activation de la sécurité pour) : *Adresse IP*	S'affiche lorsque la sécurité a été activée et que l'alerte du trap SNMP a échoué pour une adresse IP spécifiée.
Virtual Floppy connected by *User* (Disquette virtuelle connectée par *Utilisateur*)	S'affiche lorsqu'un utilisateur autorisé connecte la disquette virtuelle.

Affichage du journal d'événements	Explication
Virtual Floppy disconnected by *User* (Disquette virtuelle déconnectée par *Utilisateur*).	S'affiche lorsqu'un utilisateur autorisé déconnecte la disquette virtuelle.
License added by (Licence ajoutée par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur autorisé ajoute une licence.
License removed by (Licence retirée par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur autorisé supprime une licence.
License activation error by (Erreur d'activation de licence par) : *User (Utilisateur)*	S'affiche lorsqu'une erreur d'activation de licence se produit.
iLO 2 RBSU user login (Ouverture d'une session de l'utilitaire iLO 2 RBSU par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur autorisé ouvre une session de l'utilitaire iLO 2 RBSU.
Power on request received by (Demande de mise sous tension reçue par) : *Type*	Une demande de mise sous tension d'un des types suivants a été reçue : Power Button (Bouton de mise sous tension) Wake-On LAN (Réveil en réseau) Mise sous tension automatique
Virtual NMI selected by (NMI virtuel sélectionné par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur autorisé sélectionne le bouton NMI virtuel.
Virtual Serial Port session started by (Session de port série virtuel initiée par) : *User (Utilisateur)*	S'affiche au lancement d'une session de port série virtuel.
Virtual Serial Port session stopped by (Session de port série virtuel arrêtée par) : *User (Utilisateur)*	S'affiche lors de l'arrêt d'une session de port série virtuel.
Virtual Serial Port session login failure from (Echec d'ouverture de session de port série virtuel de) : *User (Utilisateur)*	S'affiche en cas d'échec d'une ouverture de session de port série virtuel.

Problèmes matériels et logiciels relatifs à la liaison

iLO 2 utilise un câblage Ethernet standard, et notamment CAT5 UTP avec des connecteurs RJ-45. Un câblage point à point est nécessaire pour établir une liaison matérielle vers un concentrateur Ethernet standard. Utilisez un câble croisé pour une connexion PC directe.

Le port de supervision iLO 2 doit être connecté à un réseau, lui-même connecté à un serveur DHCP, et iLO 2 doit se trouver sur le réseau avant la mise sous tension. DHCP envoie une demande aussitôt après la mise sous tension. Si la demande DHCP n'a pas reçu de réponse lors de la première initialisation de iLO 2, elle est réémise toutes les 90 secondes.

Le serveur DHCP doit être configuré pour fournir une résolution des noms DNS et WINS. La carte iLO 2 peut être configurée pour fonctionner avec une adresse IP statique soit dans la configuration de l'option F8 soit dans la page Web Network Settings (Paramètres réseau).

Le nom DNS par défaut apparaît sur l'étiquette des paramètres réseau et permet de localiser iLO 2 sans connaître l'adresse IP qui lui a été attribuée.

Si une connexion directe à un PC est employée, une adresse IP statique doit être utilisée en l'absence d'un serveur DHCP sur la liaison.

Dans l'utilitaire RBSU de iLO 2, vous pouvez appuyer sur la touche **F1** à l'intérieur de la page DNS/DHCP des options avancées pour consulter l'état des demandes DHCP de iLO 2.

Prise en charge JVM

Pour garantir le fonctionnement correct de l'applet de la console distante iLO 2 et de l'applet Virtual Media, installez Java Runtime Environment, Standard Edition 1.4.2_13. Pour localiser un lien pointant vers la dernière version prise en charge de JRE, à partir de l'interface de navigateur iLO 2, sélectionnez **Remote Console>Settings>Java** (Console distante>Paramètres>Java).

La console distante iLO 2, la console série distante et les applets Virtual Media nécessitent l'installation de JVM sur le serveur client. Si vous accédez à la console distante et aux applets Virtual Media à l'aide d'une version de Java™ Runtime Environment Standard Edition ultérieure à 1.4.2_13, les applets peuvent ne pas fonctionner correctement. Si vous utilisez une autre version de JVM, vous pouvez rencontrer les problèmes suivants :

- Si l'applet de la console distante est ouverte à l'aide de Java™ Runtime Environment, version 1.5.x ou 1.6.x, vous pouvez rencontrer les problèmes suivants :
  - Le message Automation server cannot create object (Le serveur d'automatisation ne peut pas créer l'objet) s'affiche. Si vous cliquez sur **OK**, le message disparaît et l'applet fonctionne correctement.
  - La touche TAB ne fonctionne pas correctement. La touche TAB se déplace autour des différentes parties de la fenêtre de l'applet de la console distante, et non à l'intérieur de l'applet.
- Si l'applet Virtual Media est ouverte à l'aide de Java™ Runtime Environment, version 1.5.x ou 1.6.x, vous pouvez rencontrer les problèmes suivants :
  - Lorsque vous cliquez sur le bouton **Create Disk Image** (Créer image disque), une autre fenêtre s'affiche. Dans la fenêtre qui s'affiche, les boutons Create (Créer) et Cancel (Annuler) peuvent être manquants ou s'afficher sous forme de texte uniquement. Si vous fermez et ouvrez à nouveau la fenêtre, les boutons apparaissent correctement.
  - Lorsque vous sélectionnez un fichier image dans l'applet, une fenêtre de sélection de fichier s'affiche. Après avoir sélectionné un fichier, la fenêtre se ferme et vous êtes renvoyé à la fenêtre de l'applet. Cependant, la zone du fichier image n'est pas mise à jour et l'applet ne répond pas. Pour mettre à jour la fenêtre de l'applet Virtual Media d'origine et lui permettre d'être active dans le système, cliquez sur une fenêtre séparée. L'applet ne répond pas tant que la fenêtre de l'applet Virtual Media n'a pas été fermée, puis ouverte à nouveau.

Problèmes d'ouverture de session

Utilisez les informations suivantes pour essayer de résoudre les problèmes d'ouverture de session :

- Utilisez le nom de connexion par défaut indiqué sur l'étiquette des paramètres réseau.
- Si vous oubliez votre mot de passe, un administrateur doté du privilège Administer User Accounts (Administrer comptes utilisateur) peut le redéfinir.
- Si un administrateur oublie son mot de passe, il doit utiliser le commutateur de neutralisation de la sécurité ou créer un mot de passe et un compte administrateur à l'aide de HPONCFG.
- Vérifiez les problèmes classiques :
  - Le mot de passe respecte-t-il les restrictions applicables aux mots de passe ? Par exemple, le mot de passe inclut-il des caractères majuscules et minuscules ?
  - Le navigateur utilisé est-il pris en charge ?

Nom et mot de passe d'ouverture de session refusés

Si vous vous êtes connecté à iLO 2, mais qu'il n'accepte pas votre nom et mot de passe d'ouverture de session, vous devez vérifier que les informations d'ouverture de session ont été correctement configurées. Demandez à un utilisateur doté du privilège d'administration des comptes utilisateur d'ouvrir une session, puis de changer votre mot de passe. Si vous ne parvenez toujours pas à vous connecter, demandez à l'utilisateur de rouvrir une session et de supprimer, puis de rajouter votre compte utilisateur.

REMARQUE : l'utilitaire RBSU peut également servir à corriger des problèmes d'ouverture de session.

Fermeture de session prématurée par l'utilisateur de l'annuaire

Des erreurs de réseau peuvent obliger la carte iLO 2 à conclure qu'une connexion à l'annuaire n'est plus valide. Si la carte iLO 2 ne peut pas détecter l'annuaire, elle met fin à la connexion à l'annuaire. Toutes les tentatives visant à continuer d'utiliser la connexion interrompue redirigent le navigateur sur la page de connexion.

La redirection sur la page de connexion peut correspondre une expiration de session prématurée. Une expiration de session prématurée peut se produire au cours d'une session active dans les cas suivants :

- la connexion au réseau est interrompue ;
- le serveur d'annuaire est arrêté.

Pour récupérer vos données suite à une expiration de session prématurée, connectez-vous à nouveau et continuez d'utiliser iLO 2. Si le serveur d'annuaire est indisponible, vous devez utiliser un compte local.

Accès impossible au port de supervision iLO 2 par son nom

Le port de supervision iLO 2 peut s'enregistrer sur un serveur WINS, soit un serveur DNS dynamique (DDNS) pour fournir la résolution nom-vers-adresse IP nécessaire pour accéder au port de supervision iLO 2 par le nom. Le serveur WINS ou DDNS doit être actif et en cours d'exécution avant la mise sous tension du port de supervision iLO 2 et ce dernier doit avoir un chemin valide vers le serveur WINS ou DDNS.

Il faut aussi que le port de supervision iLO 2 soit configuré avec l'adresse IP du serveur WINS ou DDNS. DHCP permet de configurer le serveur DHCP avec les adresses IP nécessaires. Vous pouvez aussi entrer les adresses IP par l'intermédiaire de l'utilitaire RBSU ou de l'option **Network Settings** (Paramètres réseau) de l'onglet Administration. Le port de supervision iLO 2 doit être configuré pour s'enregistrer sur un serveur WINS ou DDNS. Ces options sont activées par défaut et peuvent être modifiées par l'intermédiaire de l'utilitaire RBSU ou de l'option **Network Settings** (Paramètres réseau) de l'onglet Administration.

Les clients utilisés pour accéder au port de supervision iLO 2 doivent être configurés pour utiliser le même serveur DDNS que celui sur lequel l'adresse IP du port de supervision iLO 2 a été enregistrée.

Avec un serveur WINS et un serveur DNS non dynamique, l'accès au port de supervision iLO 2 peut être nettement plus rapide si vous configurez le serveur DNS afin qu'il utilise le serveur WINS pour la résolution des noms. Pour plus d'informations, reportez-vous à la documentation Microsoft® appropriée.

iLO 2 RBSU indisponible après réinitialisation du serveur et de iLO 2

Si vous réinitialisez le processeur iLO 2 et directement après le serveur, il y a un faible risque que le microprogramme de la carte iLO 2 ne soit pas totalement initialisé lorsque le serveur démarre et tente d'invoquer l'utilitaire iLO 2 RBSU. Dans ce cas, l'utilitaire iLO 2 RBSU sera indisponible ou le code ROM

de l'option de iLO 2 sera omis. Si cela se produit, réinitialisez le serveur une seconde fois. Pour éviter ce problème, laissez s'écouler quelques secondes entre la réinitialisation du processeur iLO 2 et celle du serveur.

Accès impossible à la page d'ouverture

Si vous ne parvenez pas à accéder à la page d'ouverture de session, vérifiez que le niveau de cryptage SSL est configuré à 128 bits. Le niveau de cryptage SSL dans iLO 2 est configuré à 128 bits et n'est pas modifiable. Ce niveau doit être le même sur les deux dispositifs.

Impossible d'accéder à iLO 2 via Telnet

Si vous ne parvenez pas à accéder à iLO 2 à l'aide de Telnet, vérifiez la configuration du port de console distante (paramètre Remote Console Port Configuration) et le codage des données de la console distante (paramètre Remote Console Data Encryption) dans l'écran Global Settings (Paramètres généraux). Si la configuration du port de console distante (Remote Console Port Configuration) a la valeur Automatic (Automatique), l'applet Remote Console active le port 23, lance une session et ferme le port une fois la session terminée. Telnet ne pouvant pas activer automatiquement le port 23, il échoue.

Accès impossible au support virtuel ou à la console graphique distante

Le support virtuel et la console distante graphique ne sont accessibles qu'avec la licence du pack iLO Advanced, disponible en option. Un message s'affiche pour vous informer que ces fonctions ne sont disponibles qu'avec une licence. Bien que 10 utilisateurs maximum soient autorisés à ouvrir une session iLO 2, un seul d'entre eux peut accéder à la console distante. Un message d'avertissement s'affiche pour signaler que la console distante est déjà en cours d'utilisation.

Connexion à iLO 2 impossible après la modification des paramètres réseau

Vérifiez que les deux extrémités de la connexion (carte réseau et commutateur) possèdent les mêmes paramètres de sélection automatique de la vitesse de l'émetteur récepteur, de vitesse et de duplex. Ainsi, si une extrémité est configurée pour sélectionner automatiquement la connexion, l'autre doit l'être aussi. Les paramètres de la carte réseau iLO 2 sont configurés dans l'écran Network Settings (Paramètres réseau).

Connexion impossible au port de diagnostic iLO 2

Si vous ne parvenez pas à vous connecter au port de diagnostic iLO 2 par l'intermédiaire de la carte réseau, prenez en compte les éléments suivants :

- L'utilisation du port de diagnostic est détectée automatiquement lorsqu'un câble réseau actif y est raccordé. Lors du basculement entre le port de diagnostic et le port arrière, vous devez attendre une minute environ que la commutation réseau soit exécutée avant d'essayer de vous connecter par l'intermédiaire du navigateur Web.
- Si une activité importante est en cours, le port de diagnostic est inutilisable tant que celle-ci n'est pas achevée. Les activités critiques incluent notamment :
  - mise à niveau des microprogrammes ;
  - session de la console distante ;
  - initialisation de SSL.
- Si vous utilisez une station de travail client contenant plusieurs cartes réseau activées, telles qu'une carte sans fil et une carte réseau, un problème de routage peut vous empêcher d'accéder au port de diagnostic. Pour résoudre ce problème :

1. Activez une seule carte réseau sur la station de travail client. Désactivez par exemple la carte réseau sans fil.
2. Configurez l'adresse IP du réseau du poste de travail client pour la faire correspondre au réseau du port de diagnostic iLO 2 de façon à satisfaire aux conditions suivantes :
   - Le paramètre de l'adresse IP est 192.168.1.*X*, où *X* est un nombre autre que 1, car l'adresse IP du port de diagnostic est 192.168.1.1.
   - Le paramètre du masque de sous-réseau est 255.255.255.0.

Connexion impossible au processeur iLO 2 via la carte réseau

Si vous ne parvenez pas à vous connecter au processeur iLO 2 par l'intermédiaire de la carte réseau, essayez l'une des méthodes suivantes de résolution des problèmes :

- Assurez-vous que le voyant vert (état de la liaison) du connecteur iLO 2 RJ-45 est allumé. Cela indique qu'une connexion est établie entre la carte réseau PCI et le concentrateur réseau.
- Vérifiez que le voyant vert clignote. Cela indique un trafic normal sur le réseau.
- Exécutez l'utilitaire iLO 2 RBSU pour vous assurer que la carte réseau est activée et vérifier l'adresse IP et le masque de sous-réseau qui lui ont été attribués.
- Exécutez l'utilitaire iLO 2 RBSU, puis utilisez l'onglet F1 - Advanced (F1 - Avancé) de la page DNS/DHCP pour afficher l'état des demandes DHCP.
- Testez (ping) l'adresse IP de la carte réseau à partir d'une autre station de travail du réseau.
- Essayez de vous connecter avec le navigateur en entrant l'adresse IP de la carte réseau en tant qu'URL. Vous pouvez voir la page d'accueil iLO 2 depuis cette adresse.
- Réinitialisez iLO 2.

REMARQUE : si une connexion réseau est établie, vous devrez peut-être attendre pendant 90 secondes la demande du serveur DHCP.

Les serveurs ProLiant BL p-Class proposent un port de diagnostic. Si vous connectez un câble réseau permanent au port de diagnostic, iLO 2 bascule automatiquement du port iLO 2 vers le port de diagnostic. Lors du basculement entre le port de diagnostic et le port arrière, vous devez attendre une

minute environ que la commutation réseau soit exécutée avant d'essayer de vous connecter par l'intermédiaire du navigateur Web.

Impossible de se connecter à iLO 2 après l'installation du certificat iLO 2

Si le certificat à signature automatique iLO 2 est installé de manière permanente dans certains navigateurs, et que la carte iLO 2 est réinitialisée, il peut s'avérer impossible de se reconnecter à iLO 2 car celle-ci génère un nouveau certificat à signature automatique à chaque réinitialisation. Lorsqu'un certificat est installé dans le navigateur, il est indexé par le nom qu'il contient. Ce nom est unique pour chaque iLO 2. Chaque fois que iLO 2 est réinitialisé, il génère un nouveau certificat portant le même nom.

Pour éviter ce problème, n'installez pas le certificat à signature automatique iLO 2 dans l'emplacement de stockage des certificats du navigateur. Si vous souhaitez installer le certificat iLO 2, vous devez demander un certificat permanent à une autorité de certification agréée et l'importer dans iLO 2. Ce certificat peut être installé dans l'emplacement de stockage des certificats du navigateur.

Problèmes de pare-feu

iLO 2 communique par l'intermédiaire de plusieurs ports TCP/IP configurables. Si ces ports sont bloqués, l'administrateur doit configurer le pare-feu de façon à autoriser les communications sur ces ports. Reportez-vous à la section « Administration » de l'interface utilisateur iLO 2 pour consulter ou modifier les configurations de port.

Problèmes de serveur proxy

Si votre navigateur Web est configuré pour utiliser un serveur proxy, il ne se connectera pas à l'adresse IP de la carte iLO 2. Pour résoudre ce problème, configurez le navigateur afin qu'il n'utilise pas le serveur proxy pour l'adresse IP de iLO 2. Par exemple, dans Internet Explorer, sélectionnez **Outils>Options Internet>Connexions>Paramètres du réseau local>Avancé**, puis entrez l'adresse IP ou le nom DNS de iLO 2 IP dans le champ Exceptions.

Erreur d'authentification à deux facteurs

Lorsque vous tentez d'authentifier iLO 2 à l'aide d'une authentification à deux facteurs, il se peut que vous receviez le message `The page cannot be displayed` (Impossible d'afficher la page). Ce message peut apparaître pour les raisons suivantes :

- Aucun certificat utilisateur n'est enregistré sur le système client. Pour remédier à ce problème, enregistrez le certificat utilisateur requis sur le système client. Il se peut que vous ayez besoin d'un logiciel fourni par le constructeur de la carte à puce.
- Le certificat utilisateur est stocké sur une carte à puce ou une clé USB non connectée au système client. Pour remédier à ce problème, connectez la carte à puce ou la clé USB requise au système client.
- Le certificat utilisateur n'est pas émis par l'autorité de certification agréée. Le certificat de l'autorité de certification agréée est configuré dans iLO 2 à la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs). Le certificat configuré en tant que certificat de l'autorité de certification agréée doit être le certificat public de l'autorité émettant les certificats dans votre entreprise. Pour remédier à ce problème, configurez le certificat requis en tant que certificat de l'autorité de certification agréée à la page iLO 2 Two-Factor Authentication settings ou utilisez un certificat déjà configuré émis par l'autorité de certification agréée.
- Le certificat utilisateur est expiré ou pas encore valide. Que le certificat expiré corresponde à un utilisateur local ou à un compte d'utilisateur d'annuaire, iLO 2 n'autorise pas l'authentification avec un certificat expiré ou pas encore valide. Vérifiez les dates de validité du certificat pour vous assurer

qu'il s'agit bien de la raison de l'affichage du message `The page cannot be displayed` (Impossible d'afficher la page). Pour remédier à ce problème, faites émettre un certificat valide pour l'utilisateur. Faites correspondre le certificat au compte de l'utilisateur local de iLO 2 si vous authentifiez des utilisateurs locaux et vérifiez que l'horloge de iLO 2 est correctement réglée.

- Le certificat utilisateur n'a pas été signé numériquement avec le même certificat que celui spécifié comme émanant de l'autorité de certification agréée. Bien que le nom indiqué sur le certificat de l'autorité agréée puisse correspondre à celui de l'émetteur du certificat utilisateur, il se peut que ce certificat ait été signé numériquement par un autre certificat. Vérifiez le chemin de certification du certificat utilisateur et assurez-vous que la clé publique du certificat émetteur est la même que celle du certificat de l'autorité de certification agréée. Pour remédier à ce problème, configurez le certificat requis en tant que certificat de l'autorité de certification agréée à la page iLO 2 Two-Factor Authentication settings ou utilisez un certificat émis par l'autorité de certification agréée.

Résolution des problèmes liés aux alertes et aux traps

Alerte	Explication
Test Trap (Trap de test)	Ce trap est généré par un utilisateur via la page de configuration Web.
Server Power Outage (Panne de courant du serveur)	Le serveur n'est plus alimenté.
Server Reset (Réinitialisation du serveur)	Le serveur a été réinitialisé.
Failed Login Attempt (Échec de tentative d'ouverture de session)	Une tentative d'ouverture de session à distance par un utilisateur a échoué.
General Error (Erreur générale)	Cette condition d'erreur n'est pas prédéfinie par la MIB codée en dur.
Logs (Journaux)	Le journal circulaire est saturé.
Security Override Switch Changed: On/Off (Commutateur de neutralisation de la sécurité activé/désactivé)	L'état du commutateur de neutralisation de la sécurité a changé (activé/désactivé).
Rack Server Power On Failed (Échec de la mise sous tension du serveur du rack)	Le serveur n'a pas pu être mis sous tension, car le rack BL p-Class a indiqué que l'alimentation disponible était insuffisante effectuer cette opération.
Rack Server Power On Manual Override (Neutralisation manuelle de la mise sous tension du serveur du rack)	Le client a forcé manuellement la mise sous tension du serveur bien que le rack BL p-Class ait signalé l'insuffisance de l'alimentation.
Rack Name Changed (Modification du nom du rack)	Le nom du rack ProLiant BL p-Class a été modifié.

Impossibilité de recevoir des alarmes HP SIM (traps SNMP) depuis iLO 2

Un utilisateur autorisé à configurer les paramètres iLO 2 (privilège Configure iLO 2 Settings) doit se connecter à la carte iLO 2 pour configurer les paramètres des traps SNMP. Lorsque vous êtes connecté à iLO 2, assurez-vous que les types d'alertes et les destinations de traps corrects sont activés dans l'écran SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager) de l'application de la console iLO 2.

Commutateur de neutralisation de la sécurité iLO 2

Le commutateur de neutralisation de la sécurité iLO 2 ouvre un accès d'urgence à l'administrateur avec un contrôle physique de la carte système du serveur. En activant le commutateur de neutralisation de

la sécurité iLO 2, vous disposez d'un droit de connexion, avec tous les privilèges, sans ID d'utilisateur ni mot de passe.

Le commutateur de neutralisation de la sécurité iLO 2 se trouve à l'intérieur du serveur. Vous ne pouvez dès lors pas y accéder sans ouvrir le boîtier du serveur. Pour activer le commutateur de neutralisation de la sécurité iLO 2, mettez d'abord le serveur hors tension et débranchez-le. Activez le commutateur, puis mettez le serveur sous tension. Inversez la procédure pour désactiver le commutateur de neutralisation de la sécurité iLO 2.

Un message d'avertissement s'affiche sur les pages Web iLO 2, indiquant que le commutateur de neutralisation de la sécurité iLO 2 est en cours d'utilisation. Une entrée est ajoutée au journal iLO 2 pour enregistrer l'utilisation du commutateur de neutralisation de la sécurité iLO 2. Une alerte SNMP peut également être envoyée après activation ou désactivation du commutateur de neutralisation de la sécurité iLO 2.

Dans le cas improbable où cela s'avérerait nécessaire, l'activation du commutateur de neutralisation de la sécurité iLO 2 permet également de flasher le bloc d'amorçage iLO 2. Ce dernier est alors exposé jusqu'à la réinitialisation de iLO 2. HP vous recommande de déconnecter la carte iLO 2 du réseau tant que la réinitialisation n'est pas terminée.

Suivant le serveur utilisé, le commutateur de neutralisation de la sécurité iLO 2 peut être un simple cavalier ou une position de commutateur spécifique sur un panneau de commutateurs à positions multiples. Pour y accéder, reportez-vous à la documentation de votre serveur.

Message d'erreur de code d'authentification

Sous un navigateur Mozilla, vous pouvez recevoir un message d'erreur de code d'authentification de message incorrect, vous indiquant que le code et le certificat publics ou privés utilisés pour lancer la session SSL du navigateur ont changé. Ce message d'erreur peut survenir lorsque vous n'utilisez pas de certificat fourni par le client, car la carte iLO 2 crée son propre certificat à signature automatique toutes les fois qu'elle est réinitialisée.

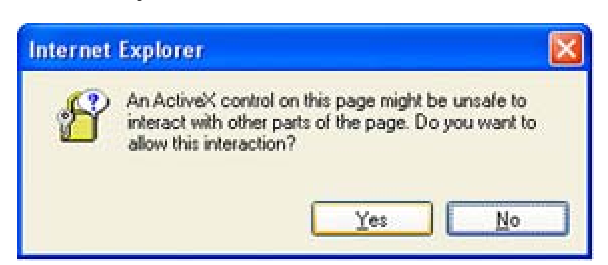
Pour résoudre ce problème, fermez et redémarrez le navigateur Web, ou installez vos propres certificats sur la carte iLO 2.

Résolution des problèmes liés à l'annuaire

Les sections suivantes expliquent comment résoudre les problèmes liés à l'annuaire.

Problèmes de connexion via le format de domaine/nom

Pour vous connecter en utilisant le format domaine/nom, les contrôles ActiveX doivent être activés. Pour vérifier que votre navigateur laisse le script de connexion appeler des contrôles ActiveX, ouvrez Internet Explorer et définissez le paramètre ActiveX sur la valeur **Prompt** (Demander). Vous devez alors voir un message semblable à celui-ci :



Les contrôles ActiveX sont activés et j'obtiens le message mais la connexion au format domaine/nom ne fonctionne pas

1. Connectez-vous avec un compte local et recherchez le nom du serveur d'annuaire.
2. Vérifiez que ce nom est bien un nom et non une adresse IP.
3. Vérifiez que vous pouvez interroger le nom du serveur d'annuaire depuis votre client avec la commande ping.
4. Exécutez des tests de configuration de l'annuaire. Vérifiez que la commande ping a été correctement reçue. Pour plus d'informations concernant les tests de paramètres d'annuaire, reportez-vous à la section « Tests d'annuaire » (Tests d'annuaire à la page 55).

Les contextes utilisateur ne semblent pas fonctionner

Contactez votre administrateur réseau. Le nom distinctif complet de votre objet utilisateur doit figurer dans l'annuaire. Votre nom de connexion correspond à ce qui apparaît après la première occurrence de CN=. Le reste du nom distinctif doit apparaître dans l'un des champs de contexte utilisateur. Les contextes utilisateur ne font pas la distinction majuscules/minuscules. Cependant, tout le reste, notamment les espaces, fait partie du contexte utilisateur.

L'utilisateur d'annuaire ne ferme pas la session après l'expiration de l'annuaire

Si vous définissez le délai d'attente de iLO 2 sur Infinite timeout (Délai d'attente illimité), la console distante interroge périodiquement le microprogramme afin de s'assurer de l'existence de la connexion. Lors de ces tests à l'aide de la commande ping, le microprogramme iLO 2 interroge l'annuaire pour obtenir la permission de l'utilisateur. Cette requête régulière permet de garder la connexion à l'annuaire active : l'utilisateur reste ainsi connecté, et tout délai est évité.

Résolution des problèmes liés à la console distante

Les sections suivantes expliquent comment résoudre les problèmes liés à la console distante. En règle générale :

- Les bloqueurs de publicité empêchent le port série virtuel et de console distante de démarrer.
- Ceux configurés pour empêcher l'ouverture automatique de nouvelles fenêtres empêchent le port série virtuel et de console distante de s'exécuter. Désactivez tous les programmes de ce type avant de démarrer le port série virtuel et de console distante.

L'applet Remote Console présente une croix rouge lorsqu'elle exécute un navigateur client Linux

Les navigateurs Mozilla doivent être configurés pour pouvoir accepter les cookies.

1. Dans le menu Préférences, sélectionnez **Confidentialité & Sécurité>Cookies**.
2. Dans l'écran Level of Privacy (Niveau de confidentialité), sélectionnez **Allow cookies based on privacy settings** (Accepter les cookies en fonction des paramètres de confidentialité), puis cliquez sur **View** (Afficher).
3. Dans l'écran Cookies, sélectionnez **Allow cookies based on privacy settings** (Accepter les cookies en fonction des paramètres de confidentialité).

Le niveau de confidentialité doit être défini sur Medium (Moyenne) ou Low (Faible).

Déplacement impossible du curseur de la console distante dans les coins de la fenêtre

Dans certains cas, il arrive que vous ne parveniez pas à déplacer le curseur de la souris dans les coins de la fenêtre de la console distante. Dans ce cas, cliquez sur le bouton droit de la souris et faites glisser le curseur en dehors de la fenêtre de la console distante, puis ramenez-le à l'intérieur de celle-ci.

Si la souris ne fonctionne toujours pas correctement, ou que le problème se produit fréquemment, vérifiez que les paramètres de la souris correspondent à ceux recommandés dans la section « Optimisation des performances de la souris pour les fonctions Remote Console (Console distante) ou Integrated Remote Console (Console distante intégrée) » (Optimisation des performances de la souris pour les fonctions Remote Console (Console distante) ou Integrated Remote Console (Console distante intégrée) à la page 99).

La console distante ne s'ouvre plus dans la session du navigateur en cours

L'ajout de la fonction Terminal Services Pass-Through (Pass-Through des services Terminal) induit un comportement de l'applet de la console distante qui est légèrement différent de ce qu'il en est dans les précédentes versions du microprogramme iLO 2. Si une session de console distante est déjà ouverte, et que vous cliquez à nouveau sur le lien de la console, la session de la console distante ne sera pas relancée. Il peut sembler à l'utilisateur que la session de la console distante s'est bloquée.

Par exemple, lorsque les étapes suivantes sont exécutées :

1. Connectez-vous à iLO 2 à partir du client-1 et ouvrez une session de console distante.
2. Connectez-vous à iLO 2 à partir du client-2 et ouvrez une session de console distante ; le message `Remote console is already opened by another session` (La console distante est déjà ouverte par une autre session) s'affiche ; ceci est tout à fait normal puisqu'il n'est possible de prendre en charge qu'une seule console distante à la fois.
3. Retournez sur le client-1 et fermez la session de console distante.
4. Cliquez sur le lien Remote Console à partir du client-2 tout en gardant ouverte l'applet de l'ancienne console distante ; la session de console distante ne s'actualise pas et l'ancien message mentionné à l'étape 2 est toujours à l'écran.

Bien qu'il soit différent de ce qu'il en était dans les versions précédentes du microprogramme iLO, c'est ce comportement qui prévaut dans la version actuelle du microprogramme iLO. Pour éviter les problèmes de cette nature, veillez à toujours fermer une session de console distante ouverte avant d'essayer de la rouvrir.

Mise à jour incorrecte de la fenêtre texte de la console distante

Lorsque vous utilisez la console distante pour afficher des fenêtres texte dont la vitesse de défilement est très rapide, il arrive que la fenêtre ne soit pas mise à jour correctement. En effet, les mises à jour de l'affichage vont trop vite pour pouvoir être détectées et affichées par le microprogramme de la carte iLO 2. En général, seul le coin supérieur gauche de la fenêtre est mis à jour, tandis que le reste demeure statique. À la fin du défilement, cliquez sur **Refresh** (Actualiser) pour mettre à jour correctement la fenêtre texte.

Ce problème se produit notamment lors des processus d'amorçage et d'auto-test de Linux, au cours desquels certains messages POST peuvent être perdus. Le processus d'amorçage peut dès lors demander d'entrer une réponse depuis le clavier. Pour éviter ce problème, HP vous recommande de ralentir le processus d'amorçage et d'auto-test en modifiant le script de démarrage de Linux afin de laisser plus de temps aux réponses en provenance du clavier.

La console distante devient grisée ou noire

L'écran de la console distante devient grisé ou noir lorsque le serveur est réinitialisé à partir du client Terminal Services. L'écran reste grisé ou noir de 30 secondes à une minute. Le client se ferme car le serveur Terminal Services est indisponible. La console distante iLO 2 devrait prendre le relais mais l'écran Remote Console (Console distante) devient grisé ou noir. Dès que l'écran redevient normal, les fonctions de la console distante sont à nouveau opérationnelles.

Résolution des problèmes liés à la console série distante

L'option Remote Serial Console (Console série distante) utilise le port série virtuel. Le port série virtuel doit être activé et correctement configuré via l'utilitaire RBSU de l'hôte. Vous pouvez accéder au port série virtuel via SSH ou Telnet (si activé). Vous pouvez accéder au CLP depuis une session de série de l'hôte si UART et le port série virtuel sont configurés de la même manière. Pour accéder au CLP depuis une session de série de l'hôte, entrez **Esc(** (échap, parenthèse gauche) pour basculer vers l'interpréteur de ligne de commande.

Les bloqueurs de fenêtres publicitaires intempestives empêcheront l'option Console série distante de fonctionner s'ils sont activés. Désactivez-les avant de lancer l'option Console série distante.

Résolution des problèmes liés à Integrated Remote Console

Les problèmes liés à Integrated Remote Console incluent :

- Problèmes liés à Internet Explorer 7
- Configuration du serveur Web Apache en vue d'une exportation
- Aucune lecture de la console lorsque le serveur est hors tension
- Omission des informations au cours de la lecture des mémoires tampons boot et fault

Internet Explorer 7 et scintillement de l'écran de console distante

L'utilisation d'Internet Explorer 7 avec la console distante peut provoquer un scintillement de l'écran de la console distante et donc des problèmes de lisibilité. Vous pouvez réduire l'effet de scintillement en définissant l'accélération matérielle du système à un niveau inférieur. Pour modifier le niveau d'accélération matérielle, allez dans **Panneau de configuration>Affichage**, puis sélectionnez l'onglet **Paramètres**. Dans la section Paramètres, cliquez sur **Avancé**. Une fois la page Avancé ouverte, cliquez sur l'onglet **Dépannage**. Baissez le niveau **Accélération matérielle** afin que l'effet de scintillement disparaisse.

Configuration Apache - Acceptation de la mémoire tampon de capture exportée

Pour garantir le bon fonctionnement de la fonction Console Replay Export (Exportation de la retransmission de la console), vous devez configurer un serveur Web de façon à accepter les données de la mémoire tampon. Vous trouverez ci-après un exemple de modification de configuration apportée à Apache, version 2.0.59 (Win32), sur un serveur exécutant Microsoft Windows Server™ 2003.

Vous devez sélectionner un emplacement de stockage pour les données exportées, définir les permissions Apache permettant d'écrire dans cet emplacement et configurer l'authentification. Pour configurer l'authentification, vous devez exécuter `htpasswd.exe` afin de créer les noms d'utilisateur et les mots de passe. Apache peut ainsi procéder à l'authentification lorsqu'il reçoit une demande d'accès à l'emplacement d'exportation. Pour plus d'informations sur la configuration des utilisateurs,

reportez-vous au site de Apache Software Foundation (http://httpd.apache.org/docs/2.0/howto/auth.html).

WebDAV propose un environnement de travail vous permettant de modifier et gérer des fichiers sur les serveurs Web. DAV, d'un point de vue technique, est une extension au protocole http. Vous devez apporter les modifications au fichier de configuration pour activer WebDAV en chargeant les modules de prise en charge Dynamic Shared Object correspondants. Les deux lignes suivantes doivent être ajoutées à la liste des modules dans le fichier `http.conf` : `LoadModule dav_module modules/mod_dav.so` et `LoadModule dav_fs_module modules/mod_dav_fs.so`.

Vous devez également activer l'authentification en chargeant les modules `LoadModule auth_module modules/mod_auth.so, LoadModule auth_digest_module modules/mod_auth_digest.so`.

Si aucun annuaire n'existe pour la base de données DavLock, vous devez en créer un. Vous avez besoin d'un annuaire DAV uniquement. Cet annuaire est référencé dans le fichier de configuration. Vous trouverez ci-après un exemple de modification de `http.conf` permettant cette prise en charge :

```
# Davlock database location
DavLockDb "C:/apache/Apache2/Apache2/dav/davlock"
# location of data being exported
Alias /images/ "C:/images/"
# Configuration of the directory to support PUT Method with authentication
<Directory "C:/images">
AllowOverride FileInfo AuthConfig Limit
AuthType Digest
# if digest is not supported by your configuration use the following
# AuthType Basic
# location of the usernames and passwords used for authentication
AuthUserFile "C:/Program Files/apache group/Apache2/passwd/passwords"
# specifies the user that is required for authentication, can be a group
# For group change to the following after creating the appropriate group
# Require group GroupName
Require user Administrator
Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
Dav On
<Limit GET PUT OPTIONS PROPFIND>
Order allow,deny
Allow from all
</Limit>
</Directory>
```

Aucune retransmission console lorsque le serveur est hors tension

La lecture des mémoires tampons de capture et les sessions de console enregistrées ne sont pas disponibles lorsque le serveur est hors tension. Vous pouvez lire les mémoires tampons capturées en les exportant sur un serveur Web et en lisant les fichiers sur une console IRC distincte du serveur. Exportez manuellement la mémoire tampon à l'aide du bouton d'exportation situé sur la page Remote Console>Settings (Console distante>Paramètres) après avoir configuré le serveur Web et l'emplacement d'exportation.

Omission des informations au cours de la lecture des mémoires tampons boot et fault

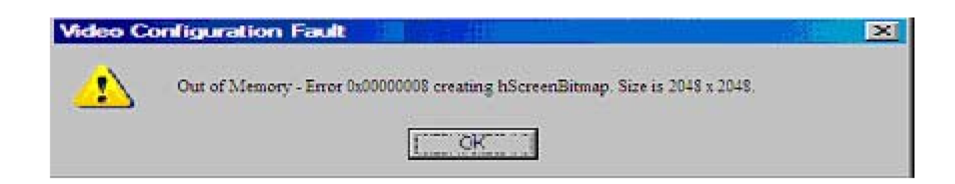
Une perte d'informations à l'écran est normale et peut se produire lors de la lecture des mémoires tampons boot et fault. Afin de résoudre le problème, assurez-vous que l'IRC est active lors des

événements boot et fault. Si vous continuez à perdre des données, essayez de capturer manuellement les séquences. Pour capturer manuellement une séquence de serveur, démarrez l'IRC et cliquez sur le bouton d'enregistrement.

Erreur de mémoire insuffisante au démarrage de Integrated Remote Console

Le système client peut manquer de mémoire si trop de sessions IRC sont ouvertes simultanément. Chaque session IRC nécessite au moins 16 MB de mémoire pour l'espace de mémoire tampon d'écran et Virtual Folder peut utiliser environ 100 MB. Si un message s'affiche au démarrage de l'IRC, la quantité de mémoire disponible sur le client est insuffisante pour mettre en mémoire tampon les données à l'écran. Par exemple :





Pour corriger ces types d'erreur, fermez certaines sessions IRC ou ajoutez de la mémoire sur l'ordinateur client afin de pouvoir ouvrir un plus grand nombre de sessions simultanément.

Le leader de session ne reçoit pas de demande de connexion lorsque l'IRC est en mode de retransmission

En tant que leader de session, lorsque vous lisez les données vidéo capturées, l'IRC n'affiche pas le message d'avertissement de type `Deny or Accept` (Refuser ou accepter) si un autre utilisateur tente d'accéder ou de partager l'IRC. La nouvelle session IRC attend et expire. Si vous demandez l'accès à l'IRC, tentez d'accéder à l'IRC et que la session expire, utilisez la fonction Acquire (Acquérir) pour prendre le contrôle de l'IRC.

Le voyant du clavier ne s'allume pas correctement

Le voyant du clavier client ne reflète pas l'état réel des différentes touches de verrouillage du clavier. Cependant, les touches Verr. Maj, Verr Num et Arrêt défil sont opérationnelles lorsque vous utilisez l'option de clavier Key Up/Down (Touche haut/bas) dans l'IRC.

IRC inactive

L'IRC iLO 2 peut devenir inactive ou être déconnectée lors de périodes d'activité intense. Le problème est signalé par une IRC inactive. Avant que l'IRC ne devienne inactive, son activité ralentit. Les symptômes d'une IRC concernée sont :

- L'affichage de l'IRC n'est pas mis à jour.
- L'activité du clavier et de la souris n'est pas enregistrée.

- Les requêtes de la console distante partagée ne sont pas enregistrées.
- La connexion Virtual Media affiche un périphérique de support virtuel vide.

Même si vous parvenez à lire un fichier capturé sur une IRC inactive, l'état actif de l'IRC n'est pas restauré.

Ce problème peut se produire lorsque plusieurs utilisateurs sont connectés à iLO 2, une session Virtual Media est connectée et effectue une opération continue de copie ou une session IRC est ouverte. L'opération continue de copie Virtual Media est prioritaire et, par conséquent, la synchronisation de l'IRC est perdue. La connexion Virtual Media est réinitialisée plusieurs fois, ce qui provoque la perte de synchronisation entre l'unité de support USB du système d'exploitation et le client Virtual Media.

Pour résoudre ce problème, reconnectez-vous à l'IRC et à Virtual Media. Si possible, réduisez le nombre de sessions utilisateur iLO 2 ouvertes simultanément. Si nécessaire, réinitialisez iLO 2 (il n'est pas nécessaire de réinitialiser le serveur).

Message d'erreur : échec de connexion de l'IRC au serveur

iLO 2 peut émettre le message `Failed to connect to server` (Échec de connexion au serveur) lorsque vous tentez d'ouvrir une session IRC. Vérifiez si la connexion Telnet est disponible.

Le client IRC iLO 2 attend pendant la durée spécifiée qu'une connexion à iLO 2 soit établie. Si le serveur client ne reçoit pas de réponse au cours de la durée spécifiée, il émet un message d'erreur.

Les causes possibles de ce message sont :

- La réponse réseau est retardée.
- Une session de console distante partagée est demandée, mais le leader de session de console distante retarde l'envoi d'un message d'acceptation ou de refus.

Pour résoudre ce problème, essayez de vous reconnecter à l'IRC. Si possible, corrigez le délai réseau et essayez de vous reconnecter à l'IRC. Si la demande concernait une session de console distante partagée, contactez le leader de session et renvoyez la demande. Si la fonction Acquire (Acquérir) de la console distante est activée, utilisez le bouton Acquire (Acquérir) plutôt que de demander une session de console distante partagée.

Les icônes de la barre d'outils IRC ne se mettent pas à jour

Lorsque vous vous connectez à l'IRC sur iLO 2, version 1.30, un objet IRC (applet de console distante iLO 2) est installé dans le navigateur. L'objet inclut les icônes de la barre d'outils pour les nouvelles fonctions proposées dans iLO2, version 1.30. Lors de l'accès à iLO 2, version 1.29 ou antérieure, l'objet IRC n'est pas remplacé par l'objet de la version du microprogramme antérieur. Par conséquent, des icônes de la barre d'outils s'affichent pour des fonctions proposées dans iLO2, version 1.30, qui ne sont pas disponibles dans les versions antérieures. Si vous cliquez sur l'une de ces icônes, un message d'erreur s'affiche.

Pour supprimer manuellement l'objet IRC, procédez comme suit :

1. Dans le navigateur Microsoft® Internet Explorer 6, cliquez sur **Outils>Options Internet**.
2. Sélectionnez **Fichiers Internet temporaires>Paramètres**.
3. Cliquez sur **Afficher les objets**.
4. Cliquez avec le bouton droit de la souris sur **iLO 2 Remote Console Applet** (Applet de console distante iLO 2), puis sélectionnez **Supprimer**.
5. Cliquez sur **OK** pour supprimer l'objet, puis sur **OK** pour fermer.

L'interface GNOME ne se verrouille pas

L'arrêt d'une console distante iLO 2 ou la perte de connectivité réseau iLO 2 ne verrouille pas l'interface GNOME si iLO 2 et l'interface GNOME sont configurés au niveau de la fonction de verrouillage de la console distante.

Le gestionnaire de clavier GNOME a besoin de temps pour traiter les séquences de touches comportant des touches de modification. Ce problème ne se produit pas lorsque les séquences de touches sont saisies manuellement via l'IRC. Le problème se pose lorsque la séquence de touches est envoyée par iLO 2. La séquence de touches comportant une touche de modification est envoyée par iLO 2 plus rapidement qu'elle n'est traitée par le gestionnaire de clavier GNOME.

Une des solutions à ce problème consiste à utiliser l'interface graphique Linux KDE à la place de GNOME. Le gestionnaire de clavier KDE n'a pas besoin de beaucoup de temps pour traiter les séquences de touches comportant des touches de modification. Les interfaces KDE et GNOME sont toutes les deux fournies avec Linux.

Répétition de touches sur la console distante

Lors de l'utilisation de la console distante pendant une période de latence du réseau, plusieurs frappes de touche peuvent être enregistrées comme une seule frappe de touche. Pour plus d'informations, reportez-vous à la section « Paramètres de la console distante » (Paramètres de la console distante à la page 91).

La lecture sur la console distante ne fonctionne pas lorsque le serveur hôte est hors tension

La lecture sur la console distante ne fonctionne pas lorsqu'elle est associée à un serveur hôte hors tension. Pour accéder à des fichiers de console distante enregistrés, mettez sous tension le serveur ou associez un iLO 2 sur un serveur sous tension.

Résolution des problèmes liés aux protocoles SSH et Telnet

Les sections suivantes expliquent comment résoudre les problèmes liés aux protocoles SSH et Telnet.

Entrée initiale dans PuTTY lente

Lors de la connexion initiale à l'aide d'un client PuTTY, l'entrée prend environ 5 secondes. Pour y remédier, modifiez les options de configuration du client sous les options de connexion TCP bas débit : décochez l'option **Disable Nagle's algorithm** (Désactiver l'algorithme de Nagle). Sous les options Telnet, définissez le mode de négociation Telnet sur **Passive** (Passif).

Le client PuTTY ne répond pas avec le port réseau partagé

Lorsque vous utilisez le client PuTTY avec le port réseau partagé, la session PuTTY peut ne pas répondre lorsqu'un volume important de données est transféré ou que vous utilisez un port série virtuel ou une console distante. Pour résoudre ce problème, fermez le client PuTT, et relancez la session.

Prise en charge SSH du mode texte à partir d'une session de la console distante

L'accès Telnet et SSH à partir de la console distante texte prend en charge la configuration standard 80 x 25 de l'écran texte. Ce mode est compatible pour la console distante texte de la majorité des interfaces texte disponibles dans les systèmes d'exploitation actuels. La configuration en mode texte

étendu supérieure à 80 x 25 ne s'affiche pas correctement lorsque vous utilisez Telnet ou SSH. HP vous recommande de configurer l'application texte en mode 80 x 25 ou d'utiliser l'applet iLO 2 Remote Console fournie par l'interface Web.

Résolution des problèmes liés aux Terminal Services

Les sections suivantes expliquent comment résoudre les problèmes liés aux Terminal Services.

Le bouton Terminal Services ne fonctionne pas

L'option Terminal Services ne fonctionne plus si l'option Deny (Refuser) est sélectionnée dans l'avertissement de sécurité de Java. Lorsque vous sélectionnez l'option Deny (Refuser), vous indiquez au navigateur que l'applet de la console distante n'est pas fiable. La console distante n'est plus autorisée à exécuter de code nécessitant un niveau supérieur de sécurité. Si l'option Deny (Refuser) est sélectionnée, la console distante ne sera pas autorisée à lancer le code requis pour activer le bouton Terminal Services. Si vous regardez dans la console Java, vous y verrez le message « `Security Exception - Access denied` » (Exception de sécurité - accès refusé).

Le serveur proxy des Terminal Services ne répond pas

À chaque réinitialisation de iLO 2 (tel que la modification des paramètres réseau ou généraux), le Pass-Through des services Terminal n'est pas disponible pendant deux minutes à compter du début de la réinitialisation. ILO 2 prend 60 secondes pour se réinitialiser et effectuer le test POST avec une mémoire tampon de 60 secondes avant de continuer. Au bout de deux minutes, l'état passe à Available (Disponible) et le Pass-Through des Terminal Services est alors utilisable.

Résolution des problèmes de vidéo et de moniteur

Les sections suivantes présentent les éléments à prendre en considération lorsque vous essayez de résoudre des problèmes de vidéo ou de moniteur.

Principes généraux

- La résolution d'écran du client doit être supérieure à celle du serveur distant.
- La console distante iLO 2 prend uniquement en charge la puce vidéo ATI Rage XL qui est intégrée au système. La fonction de console distante de iLO 2 ne fonctionne pas si vous installez une carte vidéo enfichable. Par contre, toutes les autres fonctions iLO 2 sont disponibles.
- La console distante n'est accessible qu'à un seul utilisateur à la fois. Vérifiez si un autre utilisateur a ouvert une session iLO 2.

Affichage incorrect de Telnet sous DOS®

Lorsque vous utilisez la session Telnet iLO 2 pour afficher des écrans de texte dans une fenêtre DOS® agrandie et que l'écran du serveur dépasse une taille de 80 x 25, la session Telnet ne parvient à représenter que la partie supérieure de l'écran.

Pour corriger cela, adaptez les propriétés de la fenêtre DOS® de façon à limiter sa taille à 80 x 25 avant de l'agrandir.

- Dans la barre de titre de la fenêtre DOS®, cliquez à l'aide du bouton droit de la souris et sélectionnez **Properties** (Propriétés), puis **Layout** (Mise en forme).
- Dans l'onglet Layout (Mise en forme), attribuez la valeur 25 au paramètre Screen Buffer Size (Taille du buffer d'écran).

Absence d'affichage des applications vidéo dans la console distante

Certaines applications vidéo, telles que Microsoft® Media Player, ne s'affichent pas, ou alors de manière incorrecte, dans la console distante. Ce problème est principalement rencontré avec les applications qui utilisent des registres de superposition vidéo. De façon générale, les applications qui mettent les vidéos en flux utilisent des registres de superposition vidéo. La carte iLO 2 n'est pas destinée à fonctionner avec ce type d'application.

Affichage incorrect de l'interface utilisateur

Sur les serveurs ProLiant utilisant Red Hat EL 4.0 et certains autres systèmes Linux avec iLO 2, le texte des boutons de l'interface utilisateur est parfois tronqué dans le bas du bouton. Cette erreur tient à ce que Mozilla Firefox n'affiche pas le texte à la taille spécifiée par iLO 2 pour les boutons. Afin que le texte s'affiche correctement, sélectionnez **Affichage>Taille de texte>Plus petite** jusqu'à ce que le texte s'affiche correctement.

Résolution des problèmes liés au support virtuel

Les sections suivantes expliquent comment résoudre les problèmes liés au support virtuel.

L'applet Virtual Media est signalée par un X rouge et ne s'affiche pas

L'applet Virtual Media peut être signalée par un X rouge si une JVM ou un navigateur non pris en charge est utilisé ou si l'option Enable All Cookies (Activer tous les cookies) n'est pas activée. Pour résoudre ce problème, vérifiez que vous utilisez une JVM ou un navigateur pris en charge sur votre client en consultant le tableau de support présenté dans la section « Navigateurs et systèmes d'exploitation client pris en charge » (Navigateurs et systèmes d'exploitation client pris en charge à la page 7). Assurez-vous également que la fonction Enable All Cookies (Activer tous les cookies) est sélectionnée dans le menu Options ou Preferences (Préférences) du navigateur. Certains navigateurs n'activent pas les cookies par défaut.

L'applet Virtual Floppy Media ne répond pas

L'applet iLO 2 Virtual Floppy Media peut ne plus répondre si la disquette physique contient une erreur de support.

Pour éviter ce problème, exécutez CHKDSK.EXE (ou un utilitaire du même type) afin de vérifier que la disquette ne contient pas d'erreur. Si elle en contient, rechargez l'image correspondante sur une nouvelle disquette physique.

Résolution des problèmes liés à iLO Video Player

Les sections suivantes expliquent comment résoudre les problèmes liés à iLO Video Player.

Le fichier de capture vidéo ne s'affiche pas

Vérifiez que le fichier est une capture HP iLO 2 valide, qu'il n'est pas corrompu.

La lecture du fichier de capture vidéo ne s'effectue pas correctement

Les fichiers de capture iLO 2 sont des enregistrements de l'activité de l'écran. Lorsque l'écran reste inactif pendant une durée importante, l'inactivité enregistrée est supprimée, afin de réduire la taille du fichier et d'améliorer les performances de lecture. Ce phénomène peut occasionner la lecture intermittente du fichier.

Résolution des problèmes liés à la console texte distante

Les sections suivantes présentent les éléments à prendre en considération lorsque vous essayez de résoudre des problèmes liés à la console texte distante.

Affichage du programme d'installation de Linux sur la console texte

Lorsque vous installez Linux à l'aide de la console texte, il se peut que l'écran d'installation initial ne s'affiche pas car l'écran est en mode graphique. Pour résoudre ce problème et poursuivre l'installation, effectuez l'une des opérations suivantes :

- Pour la plupart des versions de Linux, entrez `linux text nofb`. Les caractères n'apparaissent pas à l'écran. Si la commande est entrée correctement, l'écran passe du mode graphique au mode texte. L'écran peut alors s'afficher.
- Pour SLES 9 et SLES 10, appuyez sur les touches **F2** et ↓ (flèche du bas) de la console texte. Si cette action est effectuée correctement, le mode texte est sélectionné, et l'écran apparaît.

Transmission de données via un terminal SSH

Si vous utilisez un terminal SSH pour accéder à la console texte, il se peut que SSH intercepte des données de clavier, et ne transmette pas l'action à la console texte. Lorsque cela se produit, les touches du clavier semblent ne plus fonctionner. Pour résoudre ce problème, désactivez les raccourcis du terminal SSH.

Résolution de problèmes divers

Les sections suivantes expliquent comment résoudre des problèmes matériels et logiciels divers.

Cookies partagés entre les instances de navigateur et la carte iLO 2

iLO 2 utilise des cookies de navigateur pour distinguer les différentes ouvertures de session (chaque fenêtre de navigateur affiche alors une session utilisateur différente, mais la même session active est partagée avec iLO 2). Ces ouvertures de session multiples peuvent perturber le navigateur. Cette confusion peut toutefois être identifiée comme étant un problème lié à iLO 2, mais il s'agit d'un comportement classique pour un navigateur.

Plusieurs processus peuvent obliger le navigateur à ouvrir des fenêtres supplémentaires. Les fenêtres du navigateur ouvertes à partir d'un navigateur ouvert représentent différents aspects du même programme en mémoire. Par conséquent, chaque fenêtre du navigateur partage les mêmes propriétés que celles de la fenêtre parent, y compris en ce qui concerne les cookies.

Instances communes

Lorsque iLO 2 ouvre une nouvelle fenêtre du navigateur, comme par exemple Remote Console (Console distante), Virtual Media (Support virtuel) ou Help (Aide), cette fenêtre partage la même connexion à la carte iLO 2 et le cookie de la session.

Le serveur Web iLO 2 prend des décisions URL basées sur chaque requête reçue. Par exemple, si une requête ne dispose pas de privilèges d'accès, elle est redirigée vers la page de connexion, quelle que soit la requête d'origine. La redirection à partir d'un serveur Web, effectuée en sélectionnant **Fichier>Nouveau>Fenêtre** ou en appuyant sur les touches **Ctrl+N**, permet d'ouvrir une instance dupliquée du navigateur original.

Comportement de l'ordre des cookies

Durant la connexion, la page de connexion crée un cookie de navigateur qui relie la fenêtre à la session appropriée du microprogramme. Le microprogramme surveille les ouvertures de session du navigateur en tant que sessions distinctes, listées dans la section Active Sessions (Sessions actives) de la page iLO 2 Status (État de la carte iLO 2).

Par exemple, lorsque l'utilisateur User1 ouvre une session, le serveur Web génère les cadres initiaux de la vue avec l'utilisateur actuel : User1 (Utilisateur1) est dans le volet supérieur, les éléments de menu dans le volet de gauche et les données de page dans le volet inférieur droit. Au fur et à mesure que User1 clique sur les liens, seuls les éléments de menu et les données de page sont mis à jour.

Alors que User1 est connecté, si un autre utilisateur User2 (Utilisateur2) ouvre une nouvelle fenêtre de navigateur sur le même client et s'y connecte, la deuxième ouverture de session remplace le cookie généré dans la session originale de l'utilisateur User1. En supposant que User2 est un compte utilisateur distinct, un nouveau cadre est généré et une nouvelle session accordée. Le deuxième session s'affiche dans la section Active Sessions (Sessions actives) de la page iLO 2 Status (État de la carte iLO 2) avec, comme utilisateur actuel : User2 (Utilisateur2).

La deuxième ouverture de session a en effet rendu la première session (User1, Utilisateur1) orpheline, en effaçant le cookie généré pendant l'ouverture de session de User1. Ce comportement est identique à la fermeture du navigateur de User1 (Utilisateur1) sans cliquer sur le lien Log Out (Déconnexion). La session orpheline de User1 est exigée à l'expiration du délai de la session.

Le cadre de l'utilisateur actuel n'étant pas mis à jour sauf si le navigateur est obligé d'actualiser la page entière, User1 (Utilisateur1) peut continuer de naviguer en utilisant sa fenêtre de navigation. Cependant, le navigateur fonctionne à présent en utilisant les paramètres du cookie de la session de User2 (Utilisateur2), même si cela ne s'avère pas apparent.

Si User1 (Utilisateur1) continue de naviguer sous ce mode (User1 et User2 partageant le même processus du fait que User2 s'est connecté et a réinitialisé le cookie de la session), il peut se produire ce qui suit :

- La session de User1 se comporte de manière cohérente avec les privilèges affectés à User2.
- L'activité de User1 permet de maintenir la session de User2 en activité, mais la session de User1 peut s'interrompre à tout moment de façon inopinée.
- La déconnexion de l'une ou l'autre des fenêtres provoque l'arrêt des deux sessions ; l'activité suivante dans la deuxième fenêtre peut rediriger l'utilisateur sur la page d'ouverture de session, comme dans le cas d'un délai de session ou d'un délai prématuré.
- En cliquant sur Log Out from the second session (User2) (Fermeture de la seconde session [utilisateur2], le message `Logging out: unknown page to display before redirecting the user to the login page.` (fermeture de session : page inconnue à afficher avant la redirection de l'utilisateur vers la page de connexion) s'affiche.
- Si User2 se déconnecte puis se reconnecte à nouveau en tant que User3, User1 prend en charge la session de User3.
- Si User1 est en cours de connexion et User2 est déjà connecté, User1 peut changer d'URL pour être redirigé sur la page d'index. Il apparaîtra alors que User1 a accédé à iLO 2 sans s'y connecter.

Ces comportements dureront tant que les fenêtres dupliquées resteront ouvertes. Toutes les activités sont attribuées au même utilisateur, en utilisant l'ensemble de cookies de la dernière session.

Affichage du cookie de session actuel

Une fois connecté, vous pouvez obliger le navigateur à afficher le cookie de session actuel en entrant `javascript:alert(document.cookie)` dans la barre de navigation de l'URL. Le premier champ

visible est l'ID de session. Si l'ID de session est le même pour les différentes fenêtres du navigateur, ces dernières partagent une session iLO 2 commune.

Vous pouvez obliger le navigateur à actualiser et à révéler votre véritable identité en appuyant sur la touche **F5**, en sélectionnant **Affichage**>**Actualiser**, ou en utilisant le bouton Actualiser.

Prévention des problèmes utilisateur liés aux cookies

Pour éviter les problèmes de comportement basés sur les cookies :

- Lancez un nouveau navigateur pour chaque ouverture de session en double-cliquant sur l'icône du navigateur ou son raccourci.
- Cliquez sur le lien **Log Out** (Déconnexion) pour fermer la session iLO 2 avant de fermer la fenêtre du navigateur.

Impossible d'accéder aux téléchargements ActiveX

Si votre réseau n'autorise pas les contrôles ActiveX, vous pouvez récupérer le fichier DVC.DLL à partir d'un système unique et le transmettre aux machines client reliées au réseau.

1. Ouvrez une session iLO 2.
2. Saisissez **https://ilo_name/dvc.cab** dans la barre d'adresses du navigateur.
3. La boîte de dialogue de téléchargement de fichier s'affiche. Cliquez sur **Ouvrir**, puis enregistrez le fichier DVC.DLL sur votre disque dur local.
4. Copiez le fichier DVC.DLL sur le système client qui n'autorise pas les téléchargements ActiveX.
5. Depuis ce système client, ouvrez une fenêtre d'invite de commande. Accédez au répertoire contenant le fichier DVC.DLL file et saisissez `regsvr32 dvc.dll.`.

Impossible d'obtenir des informations SNMP depuis HP SIM

Les agents exécutés sur le serveur géré fournissent à HP SIM les informations SNMP. Pour que les agents puissent transférer les informations via iLO 2, les drivers de périphérique iLO 2 doivent être installés. Reportez-vous à la section « Installation des drivers de périphérique iLO 2 » pour obtenir des instructions d'installation.

Si vous avez installé les drivers et les agents pour iLO 2, vérifiez que iLO 2 et le PC de supervision se trouvent sur le même sous-réseau. Vous pouvez effectuer cette vérification rapidement en testant (ping) iLO 2 depuis le PC de supervision. Consultez votre administrateur réseau pour connaître les chemins d'accès à l'interface réseau de iLO 2.

Heure ou date incorrecte des entrées dans le journal d'événements

Vous pouvez mettre à jour la date et l'heure sur iLO 2 en exécutant l'utilitaire RBSU. Celui-ci configure automatiquement l'heure et la date du processeur en fonction de l'heure et de la date du serveur. Ces données sont également mises à jour par les agents Insight Management sur les systèmes d'exploitation réseau pris en charge.

Mise à niveau impossible du microprogramme iLO 2

Si vous tentez de mettre à niveau le microprogramme iLO 2 et que celui-ci ne répond pas, n'accepte pas la mise à niveau ou que son fonctionnement s'interrompt avant la fin de la mise à niveau, vous pouvez utiliser une des options suivantes pour restaurer votre microprogramme iLO 2. Pour plus

d'informations sur l'utilisation des possibilités de création de scripts de iLO 2, consultez le Manuel des ressources de génération de scripts et de ligne de commande.

- **Online firmware update** (Mise à jour du microprogramme en ligne) : téléchargez ce composant et exécutez-le en tant qu'administrateur ou à partir du contexte racine d'un système d'exploitation pris en charge. Ce logiciel s'exécute à partir du système d'exploitation du système hôte et met à jour le microprogramme de iLO 2 sans que vous deviez vous connecter à iLO 2.
- **Offline firmware update for SmartStart maintenance** (Mise à jour du microprogramme hors ligne pour la maintenance de SmartStart) : téléchargez ce composant pour l'utiliser avec le CD de maintenance du microprogramme de SmartStart, sous l'utilitaire de mise à jour ROM dans l'onglet Maintenance. Ces composants peuvent également être utilisés avec l'utilitaire HP Drive key boot.
- **Firmware Maintenance CD-ROM** (CD-ROM de maintenance du microprogramme) : téléchargez le composant afin de créer un CD-ROM exécutable contenant les mises à jour de plusieurs microprogrammes tels que les serveurs et les options ProLiant.
- **Scripting with CPQLOCFG** (Génération de scripts avec CPQLOCFG) : téléchargez le composant CPQLOCFG afin d'obtenir l'utilitaire de génération de scripts basé sur réseau, CPQLOCFG. CPQLOCFG permet d'utiliser des scripts RIBCL permettant l'exécution de mises à jour de microprogrammes, la configuration de iLO 2 et l'exécution par lots d'opérations pour iLO 2, et ce de façon sécurisée via le réseau. Pour les utilisateurs de Linux, vous devriez consulter le document HP Lights-Out XML PERL Scripting Samples for Linux (Exemples de scripts PERL et XML pour les périphériques HP Lights-Out pour Linux).
- **Scripting with HPONCFG** (Génération de scripts avec HPONCFG) : téléchargez le composant CPQLOCFG afin d'obtenir l'utilitaire de génération de scripts basé sur l'hôte, HPONCFG. Cet utilitaire permet d'utiliser des scripts RIBCL permettant l'exécution de mises à jour de microprogrammes, la configuration du processeur LOM et l'exécution par lots d'opérations pour ce processeur, en tant qu'administrateur ou à partir du contexte racine des systèmes d'exploitation des systèmes hôtes pris en charge.
- **HP Directories Support for Management Processors** (Prise en charge des annuaires HP pour processeurs de supervision) : téléchargez le composant pour obtenir les composants de prise en charge d'annuaires. L'un de ses composants, HPLOMIG, peut être utilisé pour localiser les processeurs iLO, iLO 2, RILOE et RILOE II et mettre à jour leur microprogramme. Il n'est pas nécessaire d'utiliser la fonction d'intégration d'annuaire pour bénéficier de cette fonctionnalité.

Étapes de diagnostic

Avant de tenter une récupération par flashage du microprogramme, vérifiez-en la nécessité à l'aide des étapes de diagnostic suivantes :

1. Essayez de vous connecter à iLO 2 par l'intermédiaire du navigateur Web. Si vous n'y parvenez pas, cela signifie qu'il y a un problème de communication.
2. Tentez de tester (PING) iLO 2. Si cela fonctionne, c'est que le réseau est opérationnel.

iLO 2 ne répond pas aux requêtes SSL

iLO 2 ne répond pas aux requêtes SSL lorsqu'un avertissement Java™ s'affiche. Si un utilisateur se connecte à une connexion du navigateur iLO 2 et interrompt le processus de connexion en répondant à l'avertissement de certificat Java™, iLO 2 ne répond pas aux requêtes ultérieures du navigateur. L'utilisateur doit poursuivre le processus de connexion pour libérer le serveur Web iLO 2.

Test de SSL

Le test suivant vérifie que l'invite de la boîte de dialogue de sécurité est correcte. Si le serveur ne fonctionne pas, le message `Page cannot be displayed` (Impossible d'afficher la page) s'affiche. En cas d'échec du test, votre contrôleur de domaine n'accepte pas les connexions SSL et n'a probablement pas reçu de certificat.

1. Ouvrez un navigateur, puis accédez à l'adresse suivante : <https://<*domain controller*> (contrôleur de domaine) : 636.

   Vous pouvez indiquer <*domain*> (domaine) au lieu de <*domain controller*> (contrôleur de domaine), qui accède au serveur DNS et vérifie quel contrôleur gère les requêtes du domaine. Testez plusieurs contrôleurs de domaine afin de vérifier qu'ils ont tous reçu un certificat.

2. Si SSL fonctionne correctement sur le contrôleur de domaine (un certificat est émis), un message de sécurité s'affiche vous demandant si vous souhaitez toujours accéder au site, ou afficher le certificat du serveur. Le fait de cliquer sur **Yes** (Oui) ne permet pas d'afficher une page Web. Ceci est normal. Ce processus est automatique, mais peut nécessiter un redémarrage. Pour éviter d'avoir à le redémarrer :

   a. Ouvrez MMC et ajoutez le composant logiciel intégrable des certificats. À l'invite, sélectionnez **Computer Account** (Compte ordinateur) pour le type des certificats à afficher. Cliquez sur **OK** pour retourner au composant logiciel intégrable des certificats.

   b. Sélectionnez le dossier **Personal>Certificates** (Personnel>Certificats). Cliquez avec le bouton droit sur le dossier et sélectionnez **Request New Certificate** (Demander nouveau certificat).

   c. Vérifiez que Type correspond au contrôleur de domaine et cliquez sur **Next** (Suivant) jusqu'à ce qu'un certificat soit utilisé.

Vous pouvez également utiliser l'outil Microsoft® LDP pour vérifier les connexions SSL. Pour plus d'informations sur l'outil LDP, visitez le site Web Microsoft® (http://www.microsoft.com/support).

Un ancien certificat peut poser les mêmes problèmes que SSL sur le pointage du contrôleur de domaine lorsqu'il pointe vers une autorité de certification agréée portant le même nom. Ce cas est rare mais peut se produire si un service de certificat est ajouté et supprimé, puis à nouveau ajouté sur le contrôleur de domaine. Pour supprimer les anciens certificats et en émettre un autre, suivez les instructions données à l'étape 2.

Réinitialisation de iLO 2

Dans certains cas rares, il peut s'avérer nécessaire de réinitialiser iLO 2, notamment lorsqu'il ne répond pas au navigateur. Pour réinitialiser iLO 2, vous devez mettre le serveur hors tension et déconnecter complètement les blocs d'alimentation.

iLO 2 peut se réinitialiser de lui-même dans certains cas. Par exemple, une horloge de surveillance iLO 2 interne se réinitialise si le microprogramme détecte un problème lié à iLO 2. iLO 2 se réinitialise aussi après une mise à niveau du microprogramme ou une modification des paramètres réseau.

La version 5.40 des agents HP Insight Management et les versions ultérieures ont la capacité de réinitialiser iLO 2. Pour ce faire, utilisez l'une des méthodes suivantes :

- Sélectionnez l'option **Reset** (Réinitialiser) de iLO 2 sur la page Web HP Management Agent (Agent de supervision HP), sous la section iLO 2.
- Pour forcer la réinitialisation manuelle du processeur de supervision de iLO 2, cliquez sur **Apply** (Appliquer) dans la page Network Settings (Paramètres réseau). Il n'est pas nécessaire de modifier des paramètres avant de cliquer sur Apply (Appliquer).
- Dans la page Diagnostic de l'interface du navigateur iLO 2, cliquez sur **Reset** (Réinitialiser).

Le nom du serveur est encore présent après l'exécution de l'utilitaire ERASE

Le champ Server Name (Nom du serveur) est communiqué à iLO 2 via les agents Insight Manager.

Pour effacer le contenu du champ Server Name (Nom du serveur) après son redéploiement, utilisez une des méthodes suivantes :

- Chargez les agents Insight Manager pour mettre à jour le champ Server Name en y entrant le nouveau nom du serveur.
- Utilisez la fonction Reset to Factory Defaults (Réinitialiser avec les valeurs d'usine) de l'utilitaire iLO 2 RBSU pour effacer le contenu du champ Server Name.

  Cette procédure efface toutes les informations de configuration iLO 2 et non seulement les informations relatives au nom du serveur.
- Modifiez le nom de serveur sur la page Administration>Access>Options (Administration>Accès>Options) de l'interface du navigateur iLO 2.

Résolution des problèmes d'un hôte distant

Pour résoudre les problèmes d'un serveur hôte distant, il peut s'avérer nécessaire de redémarrer le système distant. Pour ce faire, utilisez les options de l'onglet Virtual Devices (Périphériques virtuels).

10 Schéma des services d'annuaire

Cette section traite des rubriques suivantes :

Classes et attributs d'identificateurs d'objets (OID) LDAP centraux dans HP Management

Les modifications apportées au schéma lors de sa configuration portent sur deux types d'éléments :

- Classes centrales (Classes centrales à la page 238)
- Attributs centraux (Attributs centraux à la page 238)

Classes centrales

Nom de classe	OID affecté
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

Attributs centraux

Nom d'attribut	OID affecté
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Définitions des classes centrales

Les classes centrales de supervision HP sont définies comme suit :

hpqTarget

OID	1.3.6.1.4.1.232.1001.1.1.1.1
Description	Cette classe définit les objets cibles (Target), qui constituent la base des produits HP faisant appel à la supervision activée via l'annuaire.
Type de classe	Structurel
SuperClasses	utilisateur
Attributs	hpqPolicyDN —1.3.6.1.4.1.232.1001.1.1.2.1 hpqRoleMembership—1.3.6.1.4.1.232.1001.1.1.2.2
Commentaires	Aucun

hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
Description	Cette classe définit les objets de rôle (Role), qui constituent la base des produits HP faisant appel à la supervision activée via l'annuaire.
Type de classe	Structurel
SuperClasses	Groupe
Attributs	hpqRoleIPRestrictions—1.3.6.1.4.1.232.1001.1.1.2.5 hpqRoleIPRestrictionDefault—1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction—1.3.6.1.4.1.232.1001.1.1.2.6 hpqTargetMembership—1.3.6.1.4.1.232.1001.1.1.2.3
Commentaires	Aucun

hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Description	Cette classe définit les objets de stratégie (Policy), qui constituent la base des produits HP faisant appel à la supervision activée via l'annuaire.
Type de classe	Structurel
SuperClasses	Supérieure
Attributs	hpqPolicyDN —1.3.6.1.4.1.232.1001.1.1.2.1
Commentaires	Aucun

Définitions des attributs centraux

Les attributs de classe centraux de supervision HP sont définis comme suit :

hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1
Description	Nom distinctif de la stratégie contrôlant la configuration générale de cette cible.
Syntaxe	Nom distinctif—1.3.6.1.4.1.1466.115.121.1.12
Options	Valeur unique
Commentaires	Aucun

hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
Description	Fournit la liste d'objets cibles hpq à laquelle appartient cet objet.
Syntaxe	Nom distinctif—1.3.6.1.4.1.1466.115.121.1.12
Options	Valeur multiple
Commentaires	Aucun

hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
Description	Fournit la liste d'objets cibles hpq appartenant à cet objet.
Syntaxe	Nom distinctif—1.3.6.1.4.1.1466.115.121.1.12
Options	Valeur multiple
Commentaires	Aucun

hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Description	Chaîne booléenne représentant l'accès par des clients non spécifiés, qui indique partiellement des restrictions de privilèges sous une contrainte d'adresse réseau IP.
Syntaxe	Booléen —1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Si cet attribut est spécifié sur la valeur TRUE, les restrictions IP seront satisfaites pour les clients réseau non exceptionnels. Si cet attribut est spécifié sur la valeur FALSE, les restrictions IP seront insatisfaites pour les clients réseau non exceptionnels.

hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5
Description	Fournit une liste d'adresses IP, de noms DNS, de domaines, de plages d'adresses et de sous-réseaux qui spécifient de façon partielle des restrictions de privilèges sous une contrainte d'adresse réseau IP.
Syntaxe	Chaîne d'octets—1.3.6.1.4.1.1466.115.121.1.40
Options	Valeur multiple
Commentaires	Cet attribut est utilisé uniquement sur les objets de rôles. Les restrictions IP sont satisfaites lorsque l'adresse correspond et l'accès général est refusé, et insatisfaites lorsque l'adresse correspond et l'accès général est accordé. Les valeurs prennent la forme d'un octet d'identification suivi par un nombre d'octets de type spécifique, qui indiquent une adresse réseau. • Pour les sous-réseaux IP, l'identificateur est <0x01>, suivi de l'adresse réseau IP par ordre de réseau, elle-même suivie du masque de sous-réseau IP par ordre de réseau. Par exemple, le sous-réseau IP 127.0.0.1/255.0.0.0 serait représenté sous la forme <0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>. Pour les plages IP, l'identificateur est <0x02>, suivi par l'adresse IP inférieure liée, suivie par l'adresse IP supérieure liée. Toutes deux sont inclusives et par ordre de réseau. Par exemple, la plage IP 10.0.0.1 to 10.0.10.255 serait représentée comme <0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF>. • Pour les noms ou les domaines DNS, l'identificateur est <0x03>, suivi par le nom DNS en code ASCII. Les noms DNS peuvent être préfixés avec * (ASCII 0x2A), pour indiquer qu'ils doivent correspondre à tous les noms se terminant par la chaîne spécifiée. Par exemple, le domaine DNS *.acme.com est représenté sous la forme<0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>. L'accès général est accordé.

hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Description	Grille de temps de sept jours, avec une résolution de 30 minutes, qui spécifie les restrictions de privilège sous une contrainte de temps.
Syntaxe	Chaîne d'octets {42}—1.3.6.1.4.1.1466.115.121.1.40
Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE.

	Les restrictions de temps sont satisfaites lorsque le bit correspondant au temps local réel du périphérique est 1 et insatisfaites lorsque le bit est 0. • Le bit le moins significatif du premier octet correspond à dimanche, de minuit (00:00) à dimanche, 12:30. • Le bit suivant le plus significatif et son octet séquentiel correspondent aux blocs de demi-heure consécutifs suivants dans une même semaine. • Le bit le plus significatif, le 8ème du 42ème octet correspond à la période commençant le samedi à 22:30 jusqu'à dimanche à minuit (00:00).

Classes et attributs d'identificateurs d'objets (OID) LDAP spécifiques de la supervision Lights-Out

Le schéma suivant des attributs et des classes peut dépendre des attributs ou des classes définis dans les attributs et classes centraux de supervision HP.

Classes de supervision Lights-Out

Nom de classe	OID affecté
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

Attributs de supervision Lights-Out

Nom de classe	OID affecté
hpqLOMRightLogin	1.3.6.1.4.1.232.1001.1.8.2.1
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.6

Définitions des classes de supervision Lights-Out

Les classes centrales de supervision Lights-Out sont définies comme suit :

hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
Description	Cette classe définie les privilèges et les paramètres utilisés dans les produits HP Lights-Out Management.
Type de classe	Auxiliaire

SuperClasses	Aucun
Attributs	hpqLOMRightConfigureSettings—1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin—1.3.6.1.4.1.232.1001.1.8.2.2 hpqLOMRightLogin—1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole—1.3.6.1.4.1.232.1001.1.8.2.4 hpqLOMRightServerReset—1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia—1.3.6.1.4.1.232.1001.1.8.2.6
Commentaires	Aucun

Définitions des attributs de supervision Lights-Out

Les attributs centraux de supervision Lights-Out sont définis comme suit :

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Description	Privilège de connexion pour les produits HP Lights-Out Management.
Syntaxe	Booléen —1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Significatif uniquement pour les objets ROLE. Lorsque le paramétrage est spécifié sur TRUE, le privilège est accordé aux membres du rôle.

hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Description	Privilège de la console distante pour les produits de supervision Lights-Out. Significatif uniquement pour les objets ROLE.
Syntaxe	Booléen —1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Si l'attribut est spécifié sur TRUE, le privilège sera accordé aux membres du rôle.

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Description	Privilège du support virtuel pour les produits HP Lights-Out Management.

Syntaxe	Booléen —1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Si l'attribut est spécifié sur TRUE, le privilège sera accordé aux membres du rôle.

hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.4
Description	Privilège de réinitialisation du serveur distant et privilège du bouton d'alimentation pour les produits HP Lights-Out Management.
Syntaxe	Booléen —1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Si l'attribut est spécifié sur TRUE, le privilège sera accordé aux membres du rôle.

hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Description	Privilège administratif des bases de données de l'utilisateur local pour les produits HP Lights-Out Management.
Syntaxe	Booléen —1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Si l'attribut est spécifié sur TRUE, le privilège sera accordé aux membres du rôle.

hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Description	Privilège de configuration des paramètres de périphérique pour les produits HP Lights-Out Management.
Syntaxe	Booléen —1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Si l'attribut est spécifié sur TRUE, le privilège sera accordé aux membres du rôle.

11 Assistance technique

Cette section traite des rubriques suivantes :

Informations concernant l'assistance

Si vous avez obtenu les packs HP iLO Advanced et HP iLO Advanced pour BladeSystem en achetant les suites Insight Control et le pack iLO Power Management, vous disposez d'un service de mise à jour et une assistance technique du logiciel HP, 24h/24 7j/7, d'une durée d'un an. Ce service permet d'accéder aux ressources techniques HP afin de vous aider à résoudre les problèmes liés à la mise en œuvre ou au fonctionnement du logiciel. Ce service permet également d'accéder aux mises à jour du logiciel et aux manuels de référence soit au format électronique, soit sur support physique (en fonction de l'offre de HP).

L'assistance produit et les mises à jour sont proposées aux utilisateurs des packs HP iLO Advanced et HP iLO Advanced pour BladeSystem sous les deux formes suivantes :

- Dans le cas de licences individuelles, l'assistance technique du logiciel (démarrage) est prise en charge, sans frais supplémentaires. Il vous suffit d'appeler l'assistance HP dans un délai maximum de 90 jours à partir de la date d'achat. L'assistance téléphonique est offerte afin d'aider les clients lors des processus d'installation et de configuration, et de répondre aux questions relatives aux scripts prêts à l'emploi et à leurs diverses utilisations. Les numéros de l'assistance technique HP dans le monde sont disponibles sur le site Web HP (http://www.hp.com/country/us/en/support.html). Vous pouvez tout à fait acheter des mises à jour séparément.
- Si vous avez obtenu les packs HP iLO Advanced et HP iLO Advanced pour BladeSystem en achetant une suite Insight Control et un pack iLO Power Management, les licences incluent un service de mise à jour et une assistance technique du logiciel HP, 24h/24 7j/7, d'une durée d'un an.

  Résultat : vos problèmes sont rapidement résolus et vous recevez les dernières versions des logiciels iLO Advanced et iLO Select après avoir été informé de façon proactive de leur disponibilité. Pour plus d'informations, accédez au site Web HP (http://www.hp.com/go/ilo), sélectionnez votre produit et consultez les spécifications Quickspecs.

  Pour activer le service de mise à jour et l'assistance technique du logiciel HP pour iLO Advanced et iLO Select, vous devez enregistrer l'achat de votre logiciel via le site Web HP (http://www.hp.com/go/ilo). **L'échec d'enregistrement met en péril la prestation du service.**

  Votre SAID (Service Agreement Identifier) vous est communiqué une fois l'enregistrement terminé. Après avoir reçu votre SAID, vous pouvez accéder à la page Web du gestionnaire de mise à jour du logiciel (SUM) afin d'afficher votre contrat et de sélectionner l'envoi électronique (en plus des mises à jour sur support standard). Pour plus d'informations sur ce service, consultez le site Web HP (http://www.hp.com/services/insight).

HP propose par ailleurs divers services de support logiciel, dont bon nombre sont fournis sans frais supplémentaires.

- Assistance technique du logiciel au démarrage : une assistance téléphonique est offerte afin de répondre aux questions standard concernant l'installation, la configuration et l'utilisation du logiciel. Vous êtes ainsi mis en relation avec les spécialistes HP Insight Control Management et HP Systems Insight Manager. L'assistance est proposée sans frais supplémentaires pendant 90 jours à compter de la date d'achat du serveur. Pour obtenir une assistance aux États-Unis, appelez le
- 1-800-HP-INVENT (1-800-474-6836). (À l'invite, dites « Insight Manager , « P2P » ou « SMP ».) Les numéros de l'assistance technique HP dans le monde sont disponibles sur le site Web HP (http://www.hp.com/country/us/en/support.html).
- Forum de discussion (http://forums.itrc.hp.com) : rejoignez le forum d'assistance HP, un outil communautaire enrichi par les utilisateurs et qui permet aux clients d'échanger sur les produits HP. Pour discuter des logiciels Insight Control et Insight Essentials, cliquez sur **Management Software and System Tools** (Logiciels de supervision et outils système).
- Pages de téléchargement de logiciels et pilotes (http://www.hp.com/support) : accédez à la dernière version des logiciels et pilotes associés à vos produits ProLiant.
- Sécurité de la supervision (http://www.hp.com/servers/manage/security) : chez HP, la qualité et la sécurité de l'ensemble des logiciels de supervision sont gérées de façon proactive. Consultez régulièrement cette page afin d'accéder aux dernières versions téléchargeables des applications de sécurité.
- Dernière version de SmartStart (http://www.hp.com/servers/smartstart) : téléchargez les CD SmartStart, Management et Firmware. Il suffit de vous inscrire sur le site Web SmartStart. Si vous souhaitez recevoir les CD physiques accompagnant chaque version, vous avez la possibilité de commander individuellement les kits depuis ce même site. Pour recevoir une notification proactive lorsqu'une version de SmartStart est disponible, abonnez-vous à la e-newsletter et aux courriers électroniques (http://www.hp.com/go/subscriberschoice).

Contacter HP

Pour obtenir le nom du Revendeur Agréé HP le plus proche :

- Visitez la page Web de contacts HP dans le monde (en anglais) (http://welcome.hp.com/country/us/en/wwcontact.html).

Assistance technique HP :

- Aux États-Unis, pour connaître les options de contact, consultez la page Web de contacts HP (http://welcome.hp.com/country/us/en/contact_us.html). Pour contacter HP par téléphone :
  - Appelez le 1-800-HP-INVENT (1-800-474-6836). Ce service est disponible 24 h/24 et 7 j/7. Vos appels peuvent faire l'objet d'un enregistrement ou d'un contrôle, et ce dans le but d'améliorer en permanence la qualité du service.
  - Si vous avez acheté un Care Pack (mise à jour de service), appelez le 1-800-633-3600. Pour plus d'informations sur les Care Packs, reportez-vous au site Web HP (http://www.hp.com/hps).
- Dans les autres pays, visitez la page Web de contacts dans le monde (en anglais) (http://welcome.hp.com/country/us/en/wwcontact.html).

Avant de contacter HP

Avant d'appeler HP, munissez-vous des informations suivantes :

- Numéro d'enregistrement auprès de l'assistance technique (le cas échéant)
- Numéro de série du produit
- Nom et numéro du modèle de produit
- Numéro d'identification du produit
- Messages d'erreur obtenus, le cas échéant
- Cartes ou matériels complémentaires
- Matériel ou logiciel de fabricants tiers
- Type et niveau de version du système d'exploitation

Acronymes et abréviations

ACPI Advanced Configuration and Power Interface (Interface avancée de configuration et de courant électrique)

ARP Address Resolution Protocol (Protocole de résolution d'adresse)

ASCII American Standard Code for Information Interchange (Code américain normalisé pour l'échange d'information)

ASM Advanced Server Management (Supervision avancée de serveur)

ASR Automatic Server Recovery (récupération automatique du serveur)

BMC Baseboard management controller (Contrôleur de supervision de carte mère)

CA Certificate authority (Autorité de certification)

CLI Interface de ligne de commande

CLP Command line protocol (Protocole de ligne de commande)

CR Certificate Request (Demande de certificat)

CRL Certificate revocation list (Liste des révocations de certificat)

DAV Distributed Authoring and Versioning (Système d'auteur et de contrôle des versions distribué)

DDNS Dynamic Domain Name System (Système de noms de domaine dynamique)

DHCP Dynamic Host Configuration Protocol (protocole de configuration de serveur dynamique)

DLL Dynamic link library (Bibliothèque de liens dynamiques)

DMTF Distributed Management Task Force (Groupe de travail sur la gestion répartie)

DNS Domain Name System (Système de noms de domaine)

DVO Digital Video Out (sortie vidéo numérique)

EAAS Environment Abnormality Auto-Shutdown (Fermeture automatique pour anomalie relative à l'environnement)

EBIPA Adressage IP des baies de boîtier

EMS Emergency Management Services (Services de gestion d'urgence)

EULA End user license agreement (Contrat de licence utilisateur final ou CLUF)

FEH Fatal Exception Handler (Gestionnaire d'exceptions fatales)

GNOME GNU Network Object Model Environment

GUI Graphical User Interface (Interface utilisateur graphique)

HB Heartbeat (Message persistant)

HEM Mode High Efficiency (Mode haute efficacité)

HID Human interface device (périphérique d'interface utilisateur)

HPONCFG HP Lights-Out Online Configuration (Utilitaire de configuration en ligne HPONCFG)

HPQLOMGC HP Lights-Out Migration Command Line (Utilitaire HP de ligne de commande de migration Lights-Out)

HPQLOMIG HP Lights-Out Migration (Utilitaire HP de migration Lights-Out)

HP SIM HP SIM (Systems Insight Manager)

ICMP ICMP (Protocole de message de commande Internet)

iLO Integrated Lights-Out

iLO 2 Integrated Lights-Out 2

IML Integrated Management Log (journal de maintenance intégré)

IP Internet Protocol (Protocole Internet)

IPMI Intelligent Platform Management Interface (Interface de gestion de plate-forme intelligente)

IRC Integrated Remote Console (Console distante intégrée)

IRQ Interrupt Request (Demande d'interruption)

JVM Java Virtual Machine (Machine virtuelle Java)

KCS Keyboard Controller Style (Style de contrôleur de clavier)

KDE K Desktop Environment (environnement de bureau pour Linux)

KVM Keyboard, video and mouse (clavier, vidéo et souris)

LAN réseau local

LDAP Lightweight Directory Access Protocol

LED Light Emitting Diode (Diode émettant de la lumière)

LOM Lights-Out Management (Supervision Lights-Out)

LSB Least Significant Bit (Bit le moins significatif)

MAC (MAC) Media Access Control

MLA Master License Agreement (Accord de licence principal)

MMC Microsoft® Management Console

MP Multilink Point-to-Point Protocol (Protocole point à point multilien)

MTU Maximum Transmission Unit (Unité de transmission maximale)

NIC Network Interface Controller (Carte réseau)

NMI Non-Maskable Interrupt (Interruption non masquable)

NVRAM Mémoire non volatile

PERL Practical Extraction and Report Language (Langage PERL)

PKCS Public-Key Cryptography Standards (Normes de cryptographie à clé publique)

POST Power-On Self-Test (auto-test de mise sous tension)

PSP ProLiant Support Pack (Pack de support Proliant)

RAS Remote Access Service (Service d'accès distant)

RBSU ROM-Based Setup Utility (utilitaire de configuration basé sur la mémoire morte)

RDP Remote Desktop Protocol (Protocole de bureau à distance)

RIB Remote Insight Board (Carte Remote Insight)

RIBCL Remote Insight Board Command Language (Langage de commande de la carte Remote Insight)

RILOE Remote Insight Lights-Out Edition

RILOE II Remote Insight Lights-Out Edition II

ROM ReadOnly Memory (mémoire en lecture seule)

RSA Clé de codage public Rivest, Shamir et Adelman

RSM Remote Server Management (Supervision des serveurs à distance)

SAID Service Agreement Identifier (identifiant de l'accord de service)

SBIPC Static Bay IP Configuration (configuration IP statique)

SLES SUSE Linux Enterprise Server

SMASH System Management Architecture for Server Hardware (Architecture de la supervision du système pour le matériel du serveur)

SNMP Simple Network Management Protocol (Protocole simple de gestion de réseau)

SSH Secure Shell

SSL Secure Sockets Layer

SSO Single sign-on (authentification unique)

SUM Software update manager (gestionnaire de mise à jour du logiciel)

SUV Série, USB, vidéo

TCP Transmission Control Protocol (Protocole de contrôle de transmission)

TPM Trusted Platform Module

UART Universal asynchronous receiver-transmitter (Transmetteur récepteur asynchrone universel)

UID Unit Identification (Identification d'unité)

USB Universal Serial Bus (Bus série universel)

VM Virtual Machine

VPN Virtual Private Networking (Réseau privé virtuel)

VRM Voltage regulator module (module régulateur de tensions)

WINS Acronyme de Windows® Internet Naming Service

WS Services Web

XML eXtensible Markup Language (Langage de balisage extensible)

Index

B

C

E

F

R